Programme motion agreed to.
Written evidence (Reporting to the House) motion agreed to.
Clauses 1 to 10 agreed to, some with amendments.
Schedule 1 under consideration when the Committee adjourned till this day at Two o'clock.
No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Saturday 17 March 2018

© Parliamentary Copyright House of Commons 2018
This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright.
The Committee consisted of the following Members:

**Chairs:** †David Hanson, Mr Gary Streeter

† Adams, Nigel (Lord Commissioner of Her Majesty’s Treasury)
† Atkins, Victoria (Parliamentary Under-Secretary of State for the Home Department)
† Byrne, Liam (Birmingham, Hodge Hill) (Lab)
† Clark, Colin (Gordon) (Con)
† Elmore, Chris (Ogmore) (Lab)
† Haigh, Louise (Sheffield, Heeley) (Lab)
† Heaton-Jones, Peter (North Devon) (Con)
† Huddleston, Nigel (Mid Worcestershire) (Con)
† Jack, Mr Alister (Dumfries and Galloway) (Con)
† James, Margot (Minister of State, Department for Digital, Culture, Media and Sport)

† Jones, Darren (Bristol North West) (Lab)
† Lopez, Julia (Hornchurch and Upminster) (Con)
† McDonald, Stuart C. (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP)
† Murray, Ian (Edinburgh South) (Lab)
† O’Hara, Brendan (Argyll and Bute) (SNP)
† Snell, Gareth (Stoke-on-Trent Central) (Lab/Co-op)
† Warman, Matt (Boston and Skegness) (Con)
† Wood, Mike (Dudley South) (Con)
† Zeichner, Daniel (Cambridge) (Lab)

Kenneth Fox, Committee Clerk

† attended the Committee
Public Bill Committee

Tuesday 13 March 2018

(Morning)

[Mr David Hanson in the Chair]

Data Protection Bill [Lords]

9.25 am

The Chair: Welcome. The annunciators in the Committee Room are not working, so we will go by the Hansard clock on my left until they are repaired. I remind colleagues to switch off their mobile phones, and that tea and coffee are not permitted in Committee sittings.

Ordered,

That—

(1) the Committee shall (in addition to its first meeting at 9.25 am on Tuesday 13 March) meet—
(a) at 2.00 pm on Tuesday 13 March;
(b) at 11.30 am and 2.00 pm on Thursday 15 March;
(c) at 9.25 am and 2.00 pm on Tuesday 20 March;
(d) at 11.30 am and 2.00 pm on Thursday 22 March;
(e) at 9.25 am and 2.00 pm on Tuesday 27 March.

(2) the proceedings shall be taken in the following order:
Clauses 1 to 10; Schedule 1; Clauses 11 to 15; Schedules 2 to 4; Clauses 16 and 17; Schedule 5; Clauses 18 to 22; Schedule 6; Clauses 23 to 30; Schedule 7; Clauses 31 to 35; Schedule 8; Clauses 36 to 86; Schedules 9 and 10; Clauses 87 to 112; Schedule 11; Clauses 113 and 114; Schedule 12; Clauses 115 and 116; Schedule 13; Clauses 117 and 118; Schedule 14; Clauses 119 to 153; Schedule 15; Clause 154; Schedule 16; Clauses 155 to 181; Schedule 17; Clauses 182 to 204; Schedule 18; Clauses 205 to 208; new Clauses; new Schedules; remaining proceedings on the Bill;

(3) the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Tuesday 27 March.

—(Margot James.)

Resolved,

That, subject to the discretion of the Chair, any written evidence received by the Committee shall be reported to the House for publication.—(Margot James.)

The Chair: Copies of written evidence will be made available in the Committee Room shortly.

We now begin line-by-line consideration of the Bill. Mr Streeter—my fellow Chair—and I have selected the amendments for consideration today; the selection list is available in the Committee Room. Amendments that have been grouped for debate are generally on the same or a similar issue.

For the benefit of new Members on the Committee, I should say that decisions on amendments are made not necessarily in the order in which they are debated, as shown on the selection list, but rather in the order in which they appear on the amendment paper. Some of the provisions that we debate today will therefore not be voted on until a later day. I will use my discretion to determine whether to have separate stand part debates on clauses to which a number of amendments have been tabled. I am sure it will all become clear in due course.

Liam Byrne (Birmingham, Hodge Hill) (Lab): It is a pleasure to serve under your chairmanship, Mr Hanson. Looking around the Committee Room, I see that you have an extremely unruly bunch of hon. Members to police in the next couple of weeks, but I know that you will do so with skill and care.

The Opposition do not wish to object to clause 1, which is basically the foundation stone of the Bill. We wish only to underline the Bill’s peculiarity in that it seeks to incorporate a piece of European legislation into British law without actually reproducing the legislation in question. Throughout the debate, we will hear references to the general data protection regulation—GDPR—a text that appears nowhere in the Bill. I hope that over the coming weeks the Committee will therefore focus on a series of principles for data protection. The Opposition will move amendments to enshrine those principles more firmly into our law. Beyond that, I have no objections to this foundation stone of the Bill.

Question put and agreed to.

Clause 1 accordingly agreed to.

Clause 2

Protection of personal data

Question proposed, That the clause stand part of the Bill.

The Chair: With this it will be convenient to discuss new clause 12—Right to protection of personal data—

“(1) A person (“P”) has the right to protection of personal data concerning him or her.

(2) Personal data must be processed fairly for specified purposes as set out in the GDPR, and in accordance with the provisions, exceptions and derogations of this Act; and on the basis of the consent of P or some other legitimate basis.

(3) The Information Commissioner shall be responsible for ensuring compliance with the rights contained within this section.”

This new clause would incorporate Article 8 of the Charter of Fundamental Rights of the European Union (Protection of personal data) into the Bill.

Liam Byrne: New clause 12, which I tabled with other Opposition members of the Committee, seeks to achieve something very simple: to incorporate article 8 of the EU charter of fundamental rights into British law. It is beyond dispute that both sides of the House share the objective of ensuring friction-free trade with our neighbour, the European Union, over the years to come. The role of this Bill in enabling that trade is of fundamental
significance. Something like 70% of our exports of goods and services rely on the smooth transfer of data, and we know that the European data economy will be worth something like £643 billion by 2020. Despite all the efforts of the Secretary of State for International Trade, the reality is that the EU data economy, sitting next door to us, remains one of the most important, if not the most important, global markets from which we should aspire to profit over the years to come.

One of the great risks of Brexit is that technology firms will relocate, which is already beginning to take place. Many such firms will choose to headquarter in the Republic of Ireland. It is therefore in everybody’s interest that our trade and data protection regimes allow the smooth export of digitally enabled services. I hope that is not a contentious point.

In new clause 12, we propose to incorporate into British law what is, in effect, at the cutting edge of global data protection measures. It is not a trivial or frivolous new clause. Her Majesty’s Opposition did not make it up; it was crafted with techUK—an organisation that represents 950 companies, which employ something like 800,000 people and make up about half of the UK tech industry. When techUK proposes a fundamental measure of reform, it is important that we listen.

When we leave the European Union, we will need to agree with it an adequacy agreement by which it recognises the data protection regime in this country as adequate and therefore indicates that it is permissible for us to share data across the continental borders. The question, therefore, is how do we put that adequacy agreement beyond any doubt, not just for the immediate years after Brexit but for the decades to come? We know that trade will be fundamental to the health and wellbeing of our economy over many, many years. Let us put the data sharing regime between us and the European Union beyond doubt, not just for the short term but for the long term. Failure to get an adequacy agreement could arguably be fatal to the British economy. We simply cannot consider a shred of risk to that adequacy agreement. I hope that, having looked at this amendment and appreciated some of the refinements we made in the other place, the Government will decide that they will not put dogma in the way of agreeing to it. It is too important to leave to doubt.

In the debate on clause 1, I said that this principle was all the more important, because right hon. and hon. Members are being asked to agree to a Bill that does not feature the GDPR, which it seeks to incorporate into British law. Hon. Members can look it up if they like, but the Government have not set it out in a schedule or anywhere else. The fact that the Bill does not include the GDPR makes it all the more important that the House agrees a series of principles that are good now and for the future. Principles are paramount, and in this Bill the principle of privacy is first among equals.

The question of privacy is not disputed. It is a principle that has been agreed by our own Supreme Court in a recent case that was brought by the right hon. Member for Haltemprice and Howden (Mr Davis), who is now the Secretary of State for Brexit. Together with my hon. Friend the Member for West Bromwich East (Tom Watson), he brought the case of David Davis and others v. Secretary of State for the Home Department to the High Court, which confirmed the right of privacy in this country. This is not something that is necessarily party political; this is something on which there is strong cross-party consensus. These principles will become all the more important as the EU (Withdrawal) Bill is given effect because the Bill has thousands of ideas and proposals but kills off only one piece of legislation: the EU charter of fundamental rights.

A British tradition helped shape the EU charter of fundamental rights. We are the country of the Magna Carta and we are the country that helped craft the European convention on human rights after world war two to ensure there was never a return to the horrors of the 1930s and 1940s. Our lawyers played a fundamental role in shaping the EU fundamental charter of rights, but now, in the EU (Withdrawal) Bill, the Government decide to kill off the whole thing.

In killing off the whole thing, and in particular article 8—the fundamental foundational right to privacy—we create a new risk to keeping in lockstep the data protection regime in this country and the data protection regime in the European Union. If we bring that into doubt, we jeopardise an adequacy agreement for the future. I fear that, by setting their face against this new clause 12, the Government are, in some way and for some reason, trying to preserve the illusion of harmony between our regime and the regime of the European Union in order to camouflage the flexibility that might allow it to depart from regulatory harmonisation in the years to come. To coin a phrase, they are trying to have their cake and eat it.

That is not a reasonable position. The Minister will reassure us that that is not the intention of Her Majesty’s Government today. No doubt, she will tell us there is no will to try and win a race to the bottom in the data protection regime and many of us may be sympathetic to her position, as she is quite famously a reasonable Minister. However, the Tory party is not a stable place and the worry on all parts is not only how long the Minister will enjoy her office but what will come after her and what Government will come after this Government. There will be Governments of many colours over the course of the next 70 or 80 years and in this Committee we do not want to risk leaving unfettered a future Government who may take a less reasonable position than the famously reasonable Minister. That is why we want to move the incorporation of article 8 into British law.

We currently have a Bill without a data protection instrument and without clear data protection principles. That is a high-risk situation when, today, we have a low-risk regime. Nobody is particularly troubled by the current privacy regimes; we have been operating under article 8 of the EU charter of fundamental rights for some time and, certainly, no arguments I have heard suggest that it is troublesome in any way. What is wrong with continuing with it?

When we first crafted this new clause, there were some issues to which we were alert. A number of noble peers expressed a concern that we were creating too absolutist a right, a right without balancing test and provisions. That has been corrected in the new clause presented to this Committee today. We would therefore like to press it to a vote, as we want to ensure this fundamental right is part and parcel of British law for the years to come. It de-risks an adequacy agreement for data protection for the future. We have enjoyed the
provisions of article 8 for some years, and there is no reason to suggest that they may be more troublesome in the years ahead. We do not think the Government want to depart from a harmonisation of regulations in this area over the years to come so the flexibility that this Bill currently offers will not be taken up. Let us put the matter beyond dispute and beyond doubt and let us incorporate article 8 into the Bill.

The Chair: I remind Members—particularly new Members—that new clause 12 is being debated now, but will not be voted on, if Members wish to have a vote, until we have completed consideration of the Bill. Today's debate is on clause 2 and new clause 12, but the vote on the new clause will come later.

Brendan O'Hara (Argyll and Bute) (SNP): I rise in support of new clause 12, for two reasons. With the Bill as it stands, we see an erosion of the rights of UK citizens in a range of areas. This is particularly important because, as drafted, the EU (Withdrawal) Bill, eliminates important rights that are protected by article 8 which would otherwise constrain Ministers' ability to erode the fundamental data protection rights that we currently enjoy.

On top of that, it is essential that, post-Brexit, the United Kingdom has an adequacy agreement with the rest of the European Union. As we have heard from the right hon. Member for Birmingham, Hodge Hill, if the United Kingdom fails to secure an adequacy agreement, I fear there will be a flight of high-tech, high-skilled jobs from the United Kingdom to other parts of the European Union.

For the UK to be able to take full advantage of this vital continued free flow of data with the rest of the European Union post Brexit, the most straightforward route is an adequacy agreement. As I have heard argued before, that decision is not as straightforward as one would hope. An adequacy agreement is not simply in the Commission's gift to give; it is a legal judgment.

If I could point again to the data protection lawyer, Rosemary Jay, who said that the EU had to go through a legislative process, and it was simply not in the EU's gift to do this in any informal way. The Commission has to go through a legislative process in order to give the UK an adequacy agreement. There are further complications because, with an adequacy agreement, the European Commission has to consider a variety of issues, such as the rule of law, respect for human rights, and legislation on national public security and criminal law. That being so, it currently stands, the Investigatory Powers Act may well prove a block to achieving adequacy. The Act has already been accused of violating the European Union's charter of fundamental rights. Eduardo Ustaran, the internationally recognised expert, has said:

"What the UK needs to do is convince the Commission—and perhaps one day the European Court of Justice—that the Investigatory Powers Act is compatible with fundamental rights. That's a tall order.”

While I can understand that the Government are absolutely desperate to secure an adequacy agreement, the harsh reality is that, in these challenging circumstances and with this challenging legal process, it is not going to be as simple as perhaps we had hoped.

No one wants this situation to arise; it is absolutely essential that we have this deal, but, as GDPR evolves over time—as it surely will—in order to maintain that adequacy status, should we attain it, the UK will have to keep its data protection law in line with GDPR. The EU charter of fundamental rights and freedoms is absolutely central to EU data protection law. If we exclude ourselves now from article 8, the chances of achieving adequacy are seriously jeopardised, and the chances of maintaining adequacy are further jeopardised.

I urge the Government please to consider the long and short-term consequences of not accepting this new clause. Without article 8, I cannot see how we will achieve or maintain adequacy, and if we cannot achieve and maintain adequacy, the consequences for UK high-tech businesses are unfathomable.

Darren Jones (Bristol North West) (Lab): Thank you, Mr Hanson. It is a pleasure to serve under your chairmanship on my first Bill Committee.

I rise to support the comments made by my right hon. Friend the Member for Birmingham, Hodge Hill about the importance of adequacy and its link to article 8 of the charter of fundamental rights, and therefore in support of new clause 12. The Bill is pragmatic in seeking to bring GDPR principles into areas of non-EU competence and to provide a legislative parking space for GDPR if the UK leaves the European Union. However, we cannot get away from the fact that GDPR in itself has a legal basis that is anchored to the European charter of fundamental rights. In trying to copy and paste that level of protection into UK law, we must therefore also bring with it the fundamental rights to which it is attached.

Mike Wood (Dudley South) (Con): The hon. Gentleman is selectively quoting from that analysis. As he will see, it also says that the European Court of Human Rights—I think that the case concerned Finland—held that
article 8 of the European convention on human rights encompassed data protection rights that were protected in article 8 of the charter.

**Darren Jones:** Of course the hon. Gentleman is right that the article includes principles of data protection, but we are trying to make the Government’s job in seeking the decision on adequacy with the European Union as easy as possible. This seems an easy way to facilitate that. Clearly, there is a dereliction of fundamental rights through not copying and pasting this across into UK law. Although there are data protection principles under the European convention on human rights, article 8 states:

> “Everyone has the right to respect for his private and family life, his home and his correspondence.”

That does not sound very modern or digital to me. Although rights flow from that, the charter rights on communications—specifically electronic communications—seem much more fit for the future. I welcome the Secretary of State’s comments that the Bill seeks to make our country fit for the future. Let us not rely on a world of manual correspondence, but on one of electronic communications.

The new clause is not ideological; it does not seek to rebalance power between business controllers and individual citizens. It merely seeks to replicate what is in law today: a basic and fundamental human right that seems to me and to others to be perfectly sensible. Only yesterday, I was in Brussels with the European Scrutiny Committee, meeting Mr Barnier. He talked positively about wanting to get agreement on data adequacy, given its importance—not least because 11% of global data flows come to the UK, 70% of which are with the EU. It would be a disaster for this country if we did not have adequacy, so let us make our job easier to effect that shared aim across the Floor of the Committee and with our counterparts in Europe of seeking a decision on adequacy. Let us put this new clause into the Bill, so that we maintain the position that our data subjects have today: a fundamental right, which is in the European charter of fundamental rights, and in the future will be in this Bill.

**Margot James:** I thank speakers for their thoughtful contributions. I share many of their concerns, as do the Government, particularly with regard to adequacy, which I will talk about in more detail. I think we are all agreed that after Britain leaves the European Union we must be able to negotiate an adequacy agreement for the free flow of data between us and the EU. That is absolutely essential.

First, the GDPR implements the right to data protection and more. It is limited in scope, but the Bill also implements data protection rights on four areas beyond GDPR. It applies GDPR standards to personal data beyond EU competence, such as personal data processed for consular purposes or national security. Secondly, the Bill applies the standards to non-computerised and unstructured records held by public authorities that the GDPR ignores. Thirdly, the Bill regulates data processed for law enforcement purposes. Fourthly, it covers data processed by the intelligence services.

There is no doubt in our minds that we have fully implemented the right to data protection in our law and gone further. Clause 2 is designed to provide additional reassurance. Not only will that be clear in the substance of the legislation, but it is on the face of the Bill. The Bill exists to protect individuals with regard to the processing of all personal data. I think this is common ground. We share Opposition Members’ concern for the protection of personal data. It must be processed lawfully, individuals have rights, and the Information Commissioner will enforce them.

New clause 12 creates a new and free-standing right, which is the source of our concern. Subsection (1) is not framed in the context of the Bill. It is a wider right, not constrained by the context of EU law. However, the main problem is that it is not necessary. It is not that we disagree with the thinking behind it, but it is not necessary and might have unforeseen consequences, which I will come to.

Article 6 of the treaty on European Union makes it clear that due regard must be had to the explanations of the charter when interpreting and applying the European charter of fundamental rights. The explanations to article 8 of the charter confirm that the right to data protection is based on the right to respect for private life in article 8 of the ECHR. The European Court of Human Rights has confirmed that article 8 of the ECHR encompasses personal data protection. The Government have absolutely no plans to withdraw from the European Court of Human Rights.

The new right in new clause 12 would create confusion if it had to be interpreted by a court. For rights set out in the Human Rights Act, there is a framework within which to operate. The Human Rights Act sets out the effect of a finding incompatible with rights. However, new clause 12 says nothing about the consequences of potential incompatibility with this new right to the protection of personal data.

**Liam Byrne:** The Minister is rehearsing the argument that was made in the other place before the requirements that we put into our amendments. She can see as well as me that the new clause was rewritten so that, under subsection (2), it is to be interpreted only “in accordance with the provisions, exceptions and derogations of this Act.”

So the idea that we are creating some kind of new and unfettered right is nonsense. We had this debate in the other place. We made refinements and they have been presented in the new clause.

If there is no dispute about the importance of adequacy and of putting it beyond risk, what is the problem with putting the question beyond doubt and dispute and incorporating the same foundation that is enjoyed in the European Union into British law?

**Margot James:** New clause 12 takes article 8 of the charter outside that context and creates a free-standing right. That is the potential for confusion. New clause 12 says nothing about the consequences of incompatibility with the new right to the protection of personal data. That would create, legal, regulatory and economic uncertainty. We are endeavouring not just to ensure adequacy after we leave the European Union, but to go beyond the mere requirement for adequacy, as the Prime Minister set out in her speech almost two weeks ago.

Further, how would the courts approach other legislation in the light of this new right? One has to ask how they would approach other rights. Could this new right be balanced against other rights?
Liam Byrne: It is not a new right; it is a roll-over of an existing right. I have not heard of a case prosecuted in British courts where there was a problem with balancing the right that we currently enjoy with anything else. We simply seek to roll this right over into the future.

Margot James: That brings me on to my other point: not only does this roll-over, as the right hon. Gentleman puts it, threaten to create confusion and undermine other rights, but it is unnecessary. The charter of fundamental rights merely catalogues rights that already exist in EU law; it is not the source of those rights. The rights, including to data protection, which is importantly, what we are here to debate, arise from treaties, EU legislation and case law. They do not arise from the European charter of fundamental rights, so we argue that the new clause is completely unnecessary.

Darren Jones: The right exists in its own right in the European charter of fundamental rights. That is why European Courts refer to it when making decisions. If the Courts did not think that it was an established right in itself, they would refer to the other sources of legislation that the Minister mentioned. It therefore must, as a matter of logic, be a legal right that is fundamental; otherwise, the Courts would not refer to it.

On the Minister’s original comments about the consequences of the new clause, I think they are clear in the drafting. Subsection (2), as my right hon. Friend the Member for Birmingham, Hodge Hill said, states that processing personal data must comply with GDPR and the derogations in the Bill, and the consequences of subsection (3) are that the Information Commissioner should ensure compliance. In ensuring compliance, the commissioner will look to GDPR and the Bill to understand the consequences of a breach of a fundamental right that already exists.

Margot James: The source of the rights that we are discussing are EU legislation and case law. Those rights will be protected in UK domestic law after we leave the European Union by the European Union (Withdrawal) Bill. We have fully protected the right to data protection in our law. We have considered new clause 12 carefully, and it creates a new right. As I said, the arguments are well rehearsed, which is why we created clause 2 with the agreement of the Opposition spokespeople in the House of Lords.

The Government are determined to ensure the future free flow of data when we leave the European Union. We have heard much about the importance of, and the need for, an adequacy agreement, and I agree with everybody who has spoken on that. The general consensus is that, to achieve that, we need to faithfully implement the GDPR, and avoid the courts finding parts of the GDPR potentially incompatible with a new right. If that happened, rather than enabling the free flow of data, we would risk undermining it.

Twelve countries have negotiated adequacy arrangements with the European Union, including Canada, Israel, Uruguay, New Zealand and the United States. None of those countries was obliged by the EU Commission to put the charter of fundamental rights into their law, so I think Members can rest assured that the new clause is entirely unnecessary to achieve adequacy on our departure.

Brendan O’Hara: Does the Minister not accept that the countries she just listed were in an entirely different situation from the one that the United Kingdom finds itself in at the moment, where it is withdrawing from, rather than joining? One cannot compare like with like, because they are two entirely different situations. I believe that we are putting ourselves outside the scope of the GDPR and of achieving adequacy. The countries that she talked about took many years to achieve an adequacy agreement. The United Kingdom does not have that time. If the United Kingdom does not achieve adequacy on day one post-Brexit, does she not agree that the economy of the United Kingdom will suffer greatly as a result?

10 am

Margot James: I do not agree with the hon. Gentleman. I share his concern that we need to negotiate an adequacy agreement effectively; I am at one with him on that matter. For the reasons I have outlined, I do not believe that, if our clause is passed unamended, it will undermine that right when we come to negotiate an agreement. He made the point that those other countries are in a different position. They are already third countries in relation to us, and will be so when we leave. We will become a third country when we leave the European Union. I accept that the situation is different, but it puts us at an advantage. We are incorporating the GDPR in its entirety into UK legislation, and I assure the hon. Gentleman that we have that safeguard.

Future free flow of data is absolutely at the top of our agenda for the forthcoming EU negotiations. As I said earlier, my right hon. Friend the Prime Minister said earlier, my right hon. Friend the Prime Minister made that clear in her Mansion House speech two weeks ago. We want to secure an agreement with the EU that provides stability and confidence for EU and UK businesses and individuals, and ensures we achieve our aims of maintaining and developing the UK’s strong trading and economic links with the European Union.

Ultimately, as some Opposition Members said, importing text from the EU charter of fundamental rights is unnecessary. The general principles of EU law will be retained when we leave the EU via the European Union (Withdrawal) Bill for the purposes of the interpretation of the retained EU law. The GDPR will be retained. Indeed, the Bill will firmly entrench it in our law. The right to the protection of personal information is a general principle of EU law, and has been recognised as such since the 1960s. The withdrawal Bill requires our courts to interpret the GDPR consistently with the general principle reflected in article 8 and retained CJEU case law, so far as it is possible to do so.

Darren Jones: Does the Minister recognise that, under the European Union (Withdrawal) Bill, the application of the EU acquis—EU law—is based on legislation that existed before the point of exit? It will not continue to apply to new legislation and developments after the point of exit. The new clause needs to be in the Bill to maintain that position for the future; we must not just look back into the past.

Margot James: The European Union (Withdrawal) Bill fully protects the rights to data protection in our law. As I said earlier, we are seeking not only adequacy
after Brexit, but a continuing role in conjunction with the bodies in Europe that govern the GDPR, with the idea that we continue to contribute our expertise and benefit from theirs.

**Liam Byrne:** I am afraid we have heard a very weak argument against new clause 12. The Minister sought to prosecute two lines of argument: first, that new clause 12 risks confusion in the courts; and, secondly, that it is not needed. Let me take each in turn.

First, there can be no risk of confusion because this is not a new right. It is a right we already enjoy today, and our courts are well practised in balancing it with the other rights we enjoy. We are simply seeking to roll over the status quo into the future to put beyond doubt an adequacy agreement not just in the immediate years after we leave the European Union but in the decades that will follow.

Secondly, the Minister sought to persuade us that the new clause was not needed, and she had a couple of different lines of attack. First, she said that the source of our new protections would be the incorporation of EU case law and legislation as enshrined by the European Union (Withdrawal) Bill. Of course, that is simply not applicable to this case, because the one significant part of European legislation that the withdrawal Bill explicitly does not incorporate is the European charter of fundamental rights. The Minister slightly gave the game away when she read out the line in her briefing note that said that the rights we currently have in EU law would be enshrined and protected “so far as it is possible to do so.” That is exactly the kind of risk we are seeking to guard against.

As noble peers argued in the other place, the challenge with incorporating the GDPR into British law is that this is a piece of regulation and legislation that reflects the world of technology as it is today. It is not the first bit of data protection legislation and it will not be the last. At some point in the years to come, there will be a successor piece of legislation to this Bill and the courts’ challenge will be to make judgments that interpret an increasingly outmoded and outdated piece of legislation. We have to ensure that judgments made in the British courts and in the European courts remain in lockstep. If we lose that lockstep, we will jeopardise the future of an adequacy agreement. That will be bad for Britain, bad for British businesses and bad for technology jobs in all our constituencies.

The challenge we have with regulating in this particular field is that sometimes we have to be anticipatory in the way we structure regulations. Anyone who has spent any time with the British FinTech industry, which Ministers are keen to try and enhance, grow and develop for the years to come, will know that FinTech providers need to be able to test and reform bits of regulation in conjunction not only with the Information Commissioner but with other regulators such as the Financial Conduct Authority. For those regulators to be able to guarantee a degree of regulatory certainty, sometimes they will need to look beyond the letter of a particular piece of legislation, such as the Data Protection Bill when it becomes an Act, and reflect on the spirit of that legislation. The spirit is captured best by fundamental rights. The challenge we have is in the thousands of decisions that our regulators must take in the future. How do we put beyond doubt or dispute the preservation of regulatory lockstep with our single most important market next door?

The Uruguayan defence offered by the Minister will reassure few people. We should not be aspiring to the Uruguayan regime; we should be aspiring to something much deeper, more substantive and more harmonious.

**Liam Byrne:** My hon. Friend is right. He speaks with tremendous knowledge on this particular subject. There is a real risk that one of our most important industries will have its foundations wrecked by the inadequacies of this piece of legislation. There is no risk of confusion, there is no creation of a new and unchecked, unfettered right. We can draw no comfort from the EU (Withdrawal) Bill. There is a great risk of regulatory confusion and divergence over the years to come. I simply cannot understand why the Government would seek to put dogma and not the future protection of the British technology industry first.

This is not a trivial or frivolous issue; it has been put forward by the industry association representing half of technology jobs in this country. I hope that the Committee is persuaded by these arguments. We will seek to prosecute these arguments in a vote, at your discretion, Mr Hanson, but I hope that before we get to that point, the Government will see sense and accept the amendment.

**The Chair:** As I said, the vote on new clause 12, should there be one, will take place at a later date.

**Question put and agreed to.**

**Clause 2 accordingly ordered to stand part of the Bill.**

**Clause 3**

**TERMS RELATING TO THE PROCESSING OF PERSONAL DATA**

**Margot James:** I beg to move amendment 1, in clause 3, page 2, line 25, leave out “personal data” and insert “information”.

This amendment and Amendment 2 enable the definition of “processing” to be used in relation to any information, not just personal data.
Amendments made: 2, in clause 3, page 2, line 26, leave out “personal data, or on sets of personal data” and insert “information, or on sets of information”.

Amendment 1 agreed to.

Amendment 4, in clause 3, page 3, line 27, at end insert —
“(aa) references to Chapter 2 of Part 2, or to a provision of that Chapter, include that Chapter or that provision as applied by Chapter 3 of Part 2;”.

Amendment 5, in clause 3, page 3, line 28, leave out “processing and personal data are to processing and personal data” and insert “personal data, and the processing of personal data, are to personal data and processing”.

Amendment 6, in clause 3, page 3, line 29, at end insert —
“(c) references to a controller or processor are to a controller or processor in relation to the processing of personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies.” —[Margot James.] This amendment and amendment 3 make clear that references to controllers and processors in Parts 5 to 7 of the Bill are to controllers and processors in relation to processing to which the GDPR, the applied GDPR or Part 3 or 4 of the Bill applies.

Clause 3, as amended, ordered to stand part of the Bill.
Clauses 4 to 6 ordered to stand part of the Bill.

Amendment 62 is designed to ensure that regulations made under clause 7 will not be considered as hybrid instruments. Regulations made under the clause are already subject to the affirmative resolution procedure, and the general duty to consult before making regulations, which is set out in clause 179, also applies. In this setting, the hybrid procedure would add nothing but bureaucracy.

The amendments look like tidying-up amendments, but it would help if the Minister put on the record the extent to which they will allow the Bill to bite effectively on the nation’s schools. Obviously, schools collect a great deal of data. They often hold not only exam data but data relating to eligibility for free school meals, and most schools operate systems such as ParentPay, which means that they capture children’s biometrics. Anything to do with the protection of children’s data has to be treated incredibly seriously. The school system in this country has been balkanised—often, academies are set up as private sector entities in complex chains and have problematic governance arrangements—so I think we would all benefit from the Minister saying a few words about the Bill’s bite on schools, academies...
and colleges. Will she also say a little more about her plans to ensure that there are statutory codes of practice to which everyone who provides education services must adhere?

Margot James: I thank the right hon. Gentleman for his comments. Obviously, we share his concern about the protection of children. He cites important and highly sensitive personal data such as biometrics. Schools, like all bodies, must have a legal basis—the public interest or the normal course of their business—for processing personal data.

The right hon. Gentleman raises safeguarding. Later in our deliberations, my hon. Friend the Under-Secretary of State for the Home Department will introduce Government amendments to strengthen the safeguarding aspects of the processing of personal data. Schools are public authorities, and GDPR protections intended for authorities will apply, as I said. Schedule 3 provides further and specific protection on the points that he raises.

Liam Byrne: Will the Minister set on the record explicitly the fact that academies are covered in the same way as schools? An academy may be set up by a private sector organisation, set up as a charitable body, or set up in a way that is outwith the formal education system. Ofsted has raised concerns about unregulated schools, for example. Can she confirm whether organisations that provide education services—whether they are academies, charities or local education authority schools—are governed by the codes? Crucially, can she confirm that she will publish the code of practice?

Margot James: I certainly can confirm that the schools that the right hon. Gentleman has cited—academies run by private sector organisations and/or charities—are public authorities for the purposes of the Bill, and will be subject to the same protections.

Question put and agreed to.

Amendment made: 8, in clause 7, page 5, line 13, after “specified” insert “or described”.—(Margot James.)

See the explanatory statement for Amendment 7.

Clause 7, as amended, ordered to stand part of the Bill.

Clause 8

LAWFULNESS OF PROCESSING: PUBLIC INTEREST ETC

Daniel Zeichner (Cambridge) (Lab): I beg to move amendment 140, in clause 8, page 5, line 23, after “includes” insert “but is not limited to,”.

The Chair: With this it will be convenient to discuss amendment 141, in clause 8, page 5, line 29, at end insert “or (c) the exercise of research functions by public bodies.”

This amendment would ensure that university researchers and public bodies with a research function are able to use the “task in the public interest” lawful basis for processing personal data, where consent is not a viable lawful basis.

Daniel Zeichner: It is a pleasure to serve under your chairmanship, Mr Hanson. I shall begin by declaring an interest: I chair the all-party parliamentary group on data analytics, the secretariat to which is provided by Policy Connect. In that capacity, I have had the pleasure of having many discussions about GDPR with experts over the past couple of years. I reflect on what a good process it is that British parliamentarians in the European Parliament are able to intervene on such matters at early stages, to make sure that when the legislation finally comes to us it already has our slant on it. That may not be possible in future when we come to discuss such legislation.

I represent a university city, so research is a key part of what we do. It is on that basis that I tabled the amendments, and I am grateful to the Wellcome Trust and the Sanger Institute, which have given me advice on how the amendments would help them by providing certainty for the work that they do. The purpose of amendment 141 is to ensure that university researchers and public bodies with a research function are able to use what is called the “task in the public interest” lawful basis for processing personal data, where consent is not a viable lawful basis. I apologise for going into some detail, but it is important for universities and researchers that there is clarity.

As the Bill is drafted, clause 8 provides a definition of lawfulness of processing personal data under GDPR article 6(1)(e). Subsections (a) to (d) of clause 8 set out a narrow list of activities that could be included in the scope of public interest. I am told that that list is imported from schedule 2(5) of the Data Protection Act 1998, but I am also told that the drafters have omitted a version of the final and most general sub-paragraph from that list, which reads:

“for the exercise of any other functions of a public nature exercised in the public interest by any person.”

It is speculated that that may have been taken out of the list to tighten up, and to avoid a tautology in defining, “public interest”, but the worry is that taking it out has made the clause too restrictive. The explanatory notes indicate that the list in clause 8—that is, subsections (a) to (d)—is not intended to be exhaustive, but the Wellcome Trust and the Sanger Institute worry that it has narrowed the public interest terminology to a very narrow concept, which will be confined to public and judicial administration.

There was a very lengthy and very good debate in the other place on this matter. One of our universities’ main functions is to undertake research that will often involve processing personal data. In some cases, GDPR compliant consent, which may seem the obvious way of doing it, will not be the most appropriate lawful basis on which to process that data. It is therefore really important that an article 6 lawful basis for processing is available to university researchers with certainty and clarity.

The Government have included reference to medical research purposes in the explanatory notes, but the worry is that that does not necessarily have weight in law, and the reference excludes many other types of research that are rightly conducted by universities. This is not a satisfactory resolution to the problems that are faced.

The amendment tries to enable research functions to be conducted by public bodies such as universities without doing what the Government fear, which is to broaden the definition of “public interest” too far. The wording retains the structure of the DPA list, from which the current clauses were imported, but it narrows
it down in two ways. It specifies the purpose of processing, that is, research functions, which must be the reason for the processing and specifies who is doing the processing—the basis of it only being available to public bodies, as defined in the previous clause.

We are aware that the Government are worried about adding further subsections to the list. I think they said that it could open the floodgates in some way. However, I am told that there is not really any evidence to suggest that the current wording of paragraph 5 of schedule 2 of the Data Protection Act, which has a very broad notion of public interest, has in any way “opened the floodgates”. To give some sense of the concerns that have arisen, the processes by which university researchers seek permission to do things are quite complicated. Some of the bodies have already issued guidance. I am told that the Health Research Authority issued guidance on GDPR before Christmas. It advised that a clause on using legitimate interests should be included in the Bill.

There is confusion in the research sector, and there is a wider worry that if this is not clear, it is open to legal challenge. While some institutions will be able to take that risk, the worry is that smaller research bodies would conclude that, given the lack of clarity, it would be not be worth taking that risk. I hope that the Government will think hard about the suggestion. It comes from the research institutions themselves and would give clarity and reassurance. I hope that the Minister will accept the amendment.

Liam Byrne: I want to say a few words in support of my hon. Friend and these important amendments. I think there is an acknowledgement on both sides of the Committee that if we are to prosper in the world that is coming, we are going to need to increase the amount of money that we spend on research and development and make sure that a research-driven economy reaches every corner of the country.

The world of innovation and research is changing very quickly. I think it is next year that China becomes the world’s largest science spender for the first time in several centuries. If we are to compete in this new world, we need to invest more in our R&D base. The Government have made some helpful commitments in this area. Their proposals are not quite as ambitious as the Labour amendments, but none the less all progress is welcome.

I hope that the Minister will reflect on the reality—the way in which research is conducted in our country is changing. In the past, I have called that a shift from the cathedral to the campus. Once upon a time, big firms put a lot of people in a large building and prayed for the best. Now, they are building business parks and creating ecosystems of innovation where they may have a shared research and development facility, otherwise known as a university. There may be big international companies with global reach organised around them, but there are also scores of much smaller firms. They may be as small as a couple of post-docs in a shared lab. If we look at facilities such as BT at Dashwood Park, the Crick Institute or GSK in Stevenage, we see big global companies with hundreds of smaller companies around them which are undertaking research with much greater speed and much lower risk, but with an impact that could change the world.

We cannot jeopardise the conduct of that research. My hon. Friend the Member for Cambridge is right to point out that where there is doubt about the law, or the powers and freedoms of research firms, there is a risk that such firms simply will not undertake such work in the UK, and instead will seek relationships either with global companies or, increasingly, with universities that have R&D facilities elsewhere. We want to create the world’s best place to undertake new science, and that means having a research regime that is the best in the world. We therefore need a data protection regime that helps and does not hinder, which is why the Government should accept these carefully crafted amendments.

10.30 am

Margot James: I recognise the expertise of the hon. Member for Cambridge in this area, and I am glad of the opportunity to debate the matter fully with him, as I am conscious that I did not address the points he made in his good contribution on Second Reading. We all agree on the importance of scientific research, and one of the things I am most proud of in the industrial strategy is the huge increase in public funding for research and development. We welcome the interest in the Bill shown by the Wellcome Trust and other organisations. They are concerned that universities processing personal data in the context of ground-breaking medical research will not have a clear legal basis for doing so. The Government recognise how important that is, but we believe that the amendment is not necessary and that there is no need specifically to mention the research functions of public bodies in clause 8.

It might be helpful if I explain what clause 8 is designed to do. If an organisation is to process personal data, it must have a legal basis for doing so under article 6 of the GDPR. The clearest basis is where the data subject has given his or her consent to the processing, but article 6 also permits processing without someone’s consent in certain circumstances, including where “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”

Clause 8 helps to explain the meaning of “public interest tasks” by providing a list of processing activities that fall into that category. The list was always intended to be non-exhaustive, which is why we have used the word “includes”. In law, that word is always assumed to introduce a non-exhaustive list, and we have tried to make that point as clear as possible in the explanatory notes.

Additional phrasing in the Bill, such as that proposed in amendment 140, would add nothing to what is already in the clause’s interpretation under English law, and it would risk confusing the interpretation of the many other uses of that word elsewhere in the Bill. Given the non-exhaustive nature of the list, the fact that publicly funded research is not mentioned specifically does not mean that the research functions of public bodies will not be considered as “public interest tasks”, thereby providing a legal basis for universities to process personal data.

The Information Commissioner’s Office said: “Universities are likely to be classified as public authorities, so the public task basis is likely to apply to much of their processing”. Its guidance goes on to give “teaching and research purposes” as one such example. Hon. Members will appreciate that the list could become very long and still
not be conclusive if we included everything that the Government and the Information Commissioner’s Office consider amounts to a “public interest task”. Given those reassurances, I hope that the hon. Gentleman will not feel it necessary to press his amendment to a vote.

Daniel Zeichner: I thank the Minister for her kind words—particularly about Second Reading. I think that we were all puzzled about what was going on at about five minutes to 10; I am none the wiser. I am slightly disappointed by her response, because this is not a party political discussion. We all want to get to the same place. In many ways, the discussion we have just had is not that dissimilar from the previous one about educational institutions, schools and academies. There are many grey areas relating to what universities are, and what their status and that of the research bodies associated with them is. My worry is that if we just take the Minister’s reassurances rather than amend the Bill, the uncertainty to which I alluded—it is not my uncertainty; it is what staff at esteemed research institutions say they feel—will be a problem. We should try to improve the Bill to get the clarity we need.

The Chair: The hon. Gentleman needs to indicate to the Chair whether he wishes to withdraw the amendment or press it to a Division.

Daniel Zeichner: I think we will go to a vote, Mr Hanson. Question put, That the amendment be made.

The Committee divided: Ayes 8, Noes 10.

Division No. 1]

AYES
Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren
McDonald, Stuart C.
O’Hara, Brendan
Snell, Gareth
Zeichner, Daniel

NOES
Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel
Jack, Mr Alister
James, Margot
Lopez, Julia
Warman, Matt
Wood, Mike

Question accordingly negatived.

Margot James: I beg to move amendment 9, in clause 8, page 5, line 29, at end insert—

“( ) an activity that supports or promotes democratic engagement.”

This amendment adds a reference to processing of personal data that is necessary for activities that support or promote democratic engagement to Clause 8 (lawfulness of processing: public interest etc).

Since the Bill’s introduction, it has been brought to our attention by a range of stakeholders from all sides of the political divide that there is concern about how processing for the purpose of democratic engagement should be treated for the purposes of the GDPR. As my noble Friend Lord Ashton set out in the other place, the Government believe that there is a strong public interest in political parties and elected representatives and officials being able to engage with the public both inside and outside elections, which may sometimes include the processing of personal data.

Having considered the matter further since the debates in the other place, the Government have concluded that it would be prudent to include a provision in the Bill to provide greater clarity to those operating in the area of democratic engagement. Helpfully, clause 8 already provides high-level examples of processing activities that the Government consider could be undertaken on grounds of public interest if the data controller can demonstrate that the processing is necessary for the purposes of the processing activity. As a consequence of the importance that the Government attach to the matter, amendment 9 adds to that list

“an activity that supports or promotes democratic engagement.”

That term has been deliberately chosen with the intention of covering a range of activities carried out with a view to encouraging the general public to get involved in the exercise of their democratic rights. We think that that could include communicating with electors, campaigning activities, supporting candidates and elected representatives, casework, surveys and opinion gathering and fundraising to support any of those activities. Any processing of personal data in connection with those activities would have to be necessary for their purpose and have a legal basis. We will ensure that the explanatory notes to the Bill include such examples, to assist the interpretation of what this provision might mean in practice.

The amendment does not seek to create a partisan advantage for any one side or to create new exemptions from the data protection legislation. It is intended to provide greater clarity. It is also independent of any particular technology, given that in a short time we have moved from physical post to email, Twitter, text messages, WhatsApp, Facebook and so forth.

The Government are always open to suggestions of what else could be done to ensure legal and operational clarity for political parties and elected representatives. Further work might be needed to ensure that their current activities have the legal basis required to rely on the public interest condition. The Government will shortly engage with political parties via the parliamentary parties panel to discuss the matter further and in more detail.

Liam Byrne: I was surprised and not a little troubled that the Minister did not include the opportunity of creating Member-specific apps in her list—especially those which suck out the pictures from someone’s phone without their permission. Presumably that was not included in her list because that is already illegal.

I am grateful to the Minister for tabling the amendment and for her earlier correspondence with my noble Friend Lord Kennedy. She undertook to reflect on that correspondence and bring forward amendments. She helpfully set out a list of some of the activities that may be undertaken by a political party that fall within the ambit of the amendment. She gave a pretty comprehensive list, but will she put beyond doubt whether canvassing and collecting canvass returns were in her mind when she tabled the amendment and are therefore covered by the amendment? That would be extremely helpful.

The amendment is well intentioned. The health of our democracy is important to all parties. We look forward to the conversations that she will broker through the parliamentary parties panel.
Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): We, too, are grateful to the Minister for tabling the amendment and for her letter to you on 12 March, Mr Hanson, which has been shared with the Committee.

From our point of view, the description of democratic engagement as a new lawful basis for processing in the public interest, under article 6(1)(e) of the GDPR, is useful. In fact, there might even be an argument for including the non-exhaustive list, which I think is due to appear in the explanatory notes, in the Bill. Will the Minister think about that? I appreciate that it has been kept in very general terms.

In her letter, the Minister asked for views on whether the basis for processing data from electoral registers is currently appropriate as defined. Those registers are supplied to parties with the main condition that they are used for electoral purposes. The Law Commission, which recently reported on the review of electoral law, expressed the view that the legislation should be more precise about what that means. Again, the list in the letter that the Minister sent to you, Mr Hanson, looks like a good starting point for that.

10.45 am

The Electoral Commission has said that general political fundraising using the electoral register is not lawful, so it might be helpful to have that on the face of the Bill or in regulations. The main issue with the test of “for electoral purposes” is that every activity needs to be related to an election for it to be processed under the supplied conditions. In practice, parties engage in general campaigning, including issue-based campaigning, with the Committee.

Margot James: I thank the right hon. Member for Birmingham, Hodge Hill and his noble Friends for their constructive participation in the development of the amendment. He mentioned the app of the Secretary of State for Digital, Culture, Media and Sport; I assure him that it is compliant in every way with current data protection law and will be compliant with the provisions of the Bill. I commend my right hon. Friend for setting a new standard in the way that he communicates with his constituents.

I reassure the right hon. Member for Birmingham, Hodge Hill that canvassing and collecting canvassing returns are covered by the amendment. That is absolutely vital. I reassure the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East that it covers campaigning activity and communications between elections, concerning issues as well as elections. As I said in my short preamble, the detail of the matter can be further discussed at a meeting of the parliamentary parties panel and it is within everybody’s rights to contribute their thoughts to panel members for those important forthcoming discussions.

Amendment 9 agreed to.

Clause 8, as amended, ordered to stand part of the Bill.

Liam Byrne: The clause is an important topic of debate because it enshrines the Government’s derogation from European frameworks in law and sets the minimum age of consent for data processing at 13 rather than 16.

That derogation was invented before social media companies arrived at their current strength and delivered the very wide and sophisticated range of tools that help ensure that children become almost addicted to social media devices. In the debate on this topic over the last two or three months there have been fresh revelations from leaders of social media firms that they forbid their children to engage in the apps that their companies deliver. We have had revelations from engineers who have worked at companies such as Facebook, Twitter and Instagram that a great deal of thought goes into how they create devices and forms of interaction that encourage that basic addiction to their apps.

We are at the beginning of what I hope is a period of re-regulation and better regulation of these firms, so that we can do away with many of the risks that affect our children. In a way, I was encouraged to see the Secretary of State’s interview with The Times on Saturday, in which he said very clearly that he would like to see better regulation of social media firms in this country before his own children are tempted to engage in this exciting online world. Many of us have children who are already engaged in this and, as a parent, I have real concerns about the freedom with which social media companies can develop and deliver these techniques, as well as their freedom to take a rather relaxed view of taking down often unfortunate and extremist content. I know that we will have this debate later, and we have tabled amendments to encourage the Government to set a deadline for reforming the electronic commerce directive.

It is important to draw a little more out of the Government about how they see the safeguards coming into place around clause 9. We have not sought to challenge the derogation the Government seek to enshrine in the Bill, but we ensured widespread support for Baroness Kidron’s amendment on the creation of an age-appropriate code. However, rather than simply wave clause 9 through, it is incumbent on the Minister to say a little about how she will ensure that there are adequate safeguards in place to protect our children from the very threats the Secretary of State lit up in lights on Saturday.

Margot James: I support the general tone of the right hon. Gentleman’s comments. I too was pleased to see the interview with the Secretary of State, his focus on the addictive nature of some of these apps and the idea that there could be within the technology a means of limiting the time children spend on them, which parents could click on. The Information Commissioner’s Office will publish guidance shortly on how clause 9 will work and what those safeguards will be. She will take into consideration an age-appropriate design, as suggested by Baroness Kidron.

Overall, where online services referred to in the Bill as “information society services” choose to rely on consent as the basis for their processing, article 8 of the GDPR sets the age below which a website must obtain the parents’ and not the child’s consent. Most websites will be captured by this additional safeguard, ranging from online banking to search engines to social media, with social media probably being the most relevant to the age group in question.
The GDPR gives member states the flexibility to set this age within a prescribed range of between 13 and 16. The Bill sets it at 13, with an exception for preventive and counselling services, for which the test is based purely on the child’s capacity to understand what they are being asked to consent to. The Government are satisfied that the Information Commissioner’s Office has adequate enforcement powers, including large fines for any offences committed in this area.

**Darren Jones:** The Minister said that Europe provides that the age range is between 13 and 16. In fact, the GDPR says the age for consent is 16, but that member states can derogate down to 13. I do not wish to be an annoying lawyer, but it is an important distinction. Our colleagues in Europe are saying that the age they deem to be appropriate is 16, but they are giving member states flexibility to go lower. Interestingly, article 8(2) talks about how reasonable efforts need to be taken to verify age and consent “taking into consideration available technology.”

My view is that, on these types of issues, there should be better technology for age verification as part of using online services and, where children’s data is being used to commercialise and monetise for the purposes of advertising, there should be additional safeguards for children.

I ask the Minister only to keep an open mind in the future, so that when we get to a position where technology providers can verify the age of children—I appreciate that is perhaps currently a little difficult—if industry does not move voluntarily to this position, the Government consider regulating in that regard.

**Margot James:** The hon. Gentleman is right that the GDPR stipulates 16 as the minimum age for consenting to data processing without parental consent, but that it provides for member states to derogate from that. At least seven, including Spain, Ireland and Denmark, have done just that. Like us, they have proposed a much younger age of 13, so we are not an outlier on the issue.

Currently, the minimum age in this country for allowing personal data to be used without parental consent is 12, so in a sense we are derogating from that policy by setting the minimum age at 13 in the Bill. The hon. Gentleman is right to point out that it is very difficult for technology companies to implement meaningful verification mechanisms for those younger than 18, who may not have anything like a credit card or driving licence. I have no doubt that the Government will keep an open mind on the matter, in line with other developments that will take place long after the Bill is passed.

*Question put and agreed to.*

Clause 9 accordingly ordered to stand part of the Bill.

**Clause 10**

**SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL CONVICTIONS ETC DATA**

**Stuart C. McDonald:** I beg to move amendment 129, in clause 10, page 6, line 19, leave out subsections (6) and (7).

*This amendment would remove delegated powers that would allow the Secretary of State to vary the conditions and safeguards governing the general processing of sensitive personal data.*

The Chair: With this it will be convenient to discuss the following:

Amendment 132, in clause 35, page 21, line 29, leave out subsections (6) and (7).

*This amendment would remove delegated powers that would allow the Secretary of State to vary the conditions and safeguards governing the general processing of sensitive personal data.*

Amendment 134, in clause 86, page 50, line 33, leave out subsections (3) and (4).

*This amendment would remove delegated powers that would allow the Secretary of State to vary the conditions and safeguards governing the general processing of sensitive personal data.*

**Stuart C. McDonald:** The amendments stand not only in my name and that of my hon. Friend the Member for Argyll and Bute, but in the names of Labour Members, for whose support we are very grateful.

There cannot be anyone in this Committee Room who does not know what a Henry VIII power is. If my email inbox is anything to go by, half the country knows what a Henry VIII clause is now, even if they did not know before the European Union (Withdrawal) Bill commenced its progress through the House. Amendments 129, 132 and 134 would remove Henry VIII powers from clauses 10, 35 and 86 respectively. To explain why those powers are not appropriate and need to be removed, I need to explain briefly what those clauses concern and why the powers are therefore too significant and wide.

Clause 10 needs to be read alongside article 9 of the GDPR, which states unambiguously:

“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.”

Such data includes some of the most sensitive information that we can imagine. Article 9 then sets out situations in which the prohibition does not apply. Some of the exceptions that it lists, such as those in which “processing relates to personal data which are manifestly made public by the data subject”, apply directly, so the Bill need not address them. Others need to be interpreted in accordance with EU or member state law before they can be relied on; for instance, paragraph 2(g) of article 9 states that the prohibition shall not apply if “processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law”.

Clause 10, which applies schedule 1, establishes the basis in member state law for lifting the prohibition on processing such sensitive information. For example, part 2 of schedule 1 includes 18 conditions—ranging from parliamentary and ministerial functions to preventing money laundering and detecting unlawful acts—that provide the basis in UK law for the substantial public interest exception to apply to the processing of special categories of personal data.

Clause 35 is in part 3, which is headed “Law enforcement processing”. It states that the first of the data protection principles by which law enforcement bodies must abide is that the processing of personal data for any of the law enforcement purposes must be lawful and fair. The specific conditions that must be met with respect to sensitive data are set out in schedule 8, which is similar to schedule 1. They include cases in which the processing is necessary...
"for the administration of justice"

or

"to protect the vital interests of the data subject or of another individual."

Clause 86 is in part 4, “Intelligence services processing”. It essentially does for that activity what clause 35 does for law enforcement, and it applies schedule 10. In short, we have a carefully framed set of exceptions to the prohibition on processing of this extremely sensitive information, and those exceptions provide a lawful basis for the processing of information that we normally would not dream of processing because of its highly intrusive and sensitive nature.

11 am

There should always be a presumption against Henry VIII clauses, and that is definitely the case when we are talking about such sensitive information. There are fine balances to be struck between the right to privacy and the necessity of our law enforcement agencies, intelligence services and other bodies being able to process that information. The Bill seeks to strike that balance very finely.

It would therefore be inappropriate to give the Government the power to hand out new powers to process sensitive data without proper scrutiny and the ability of parliamentarians in this place to amend such proposals. It would be completely inappropriate to do it by all or nothing, “accept or reject” statutory instrument procedures. Any adjustments to this fine balance deserve the greatest of scrutiny; we on this Bill Committee are essentially wasting our time if we are just handing the Government a blank cheque to hand out powers as and when they see fit. We seek support for our amendments to remove these Henry VIII powers from the Bill.

Liam Byrne: We support these amendments very strongly, and if possible we would like to test the Committee’s will on this. The Bill has a succession of Henry VIII powers at a number of different clauses, which in effect give the Secretary of State the power to vary and amend regulations that are incredibly important. We cannot detach this debate from the earlier debate on the incorporation of article 8. We now have a Bill that is pretty weak on the fundamental principles of law that it seeks to enshrine; the Government want to set their face against incorporating some protections that we have in the European charter of fundamental rights. Therefore, the idea that we leave out some fundamental protections of rights, but then hand over to the Minister unfettered power to make regulations as he or she sees fit, does not seem to be in Parliament’s best interest. We think that the Government need to think again.

The powers in this particular clause create the possibility that exemptions to data protection rights, which have not been considered or debated in Parliament, go through effectively at the whim of the Minister. Those powers are enshrined in clause 10, and in clauses 35 and 86; we will come on to those debates, but the powers that clause 10 proposes to grant the Minister are in effect unilaterally to vary the conditions and safeguards governing the general processing of sensitive personal data—the general data set out in schedule 1—and then to add new conditions to schedules 1, 8 and 10.

That means that we would basically give the Secretary of State the power to expand the permissible reasons to allow processing of sensitive personal data, both generally and particularly for law enforcement and intelligence agencies. That is something that has been considered extensively in the other place. The House of Lords Constitution Committee said:

“The Government’s desire to future-proof legislation...must be balanced against the need for Parliament to scrutinise and, where necessary, constrain executive power.”

The Delegated Powers and Regulatory Reform Committee said that

“it is not good enough for Government to say that they need ‘flexibility’ to pass laws by secondary instead of primary legislation without explaining in detail why”.

The Ministers slightly let the cat out of the bag when Baroness Chisholm spoke up for the Government and said that if they were to accept the Committee’s recommendations in full that would

“leave the Government unable to accommodate developments in data processing and the changing requirements of certain sectors”—

[Official Report, House of Lords, 11 December 2017; Vol. 787, c. 1464.]

That includes, for example, the insurance sector. That is patently nonsense. It would not constrain the Government’s ability to introduce wise regulations in this place; it would simply constrain the Government’s ability to do that unilaterally without effective recourse to Parliament.

We are seeking a very clear Government explanation as to why the Secretary of State, not Parliament, should be empowered to alter the data protection regime to keep it up to date, and that explanation needs to be all the more robust following the remarks that the Minister has made about her attitude towards incorporating the fundamental right of privacy in British law.

We think that the amendments would be sensible constraints on Henry VIII powers. There is wide consensus across both Houses that they are necessary. They will not damage or diminish the Secretary of State’s ability to keep regulation up to date. Many of us have been in this place long enough to know that it is perfectly within the Executive’s power to keep regulatory reform on track if the political will is there. We are asking for a defence of Parliament’s right to oversee, scrutinise and, where necessary, constrain the powers of the Secretary of State to regulate in this field.

Margot James: Following recommendations by the Delegated Powers and Regulatory Reform Committee, we have considered carefully the use of the Bill’s order-making powers and amended the Bill in the House of Lords to provide additional safeguards for the exercise of those powers, but Members of the Lords on all sides of the House agreed that it was essential to retain the order-making powers in the Bill as amended.

I will explain how the powers will be used in practice. Article 9 of the GDPR prohibits the processing of special categories of personal data unless one of the exemptions in paragraph 2 of article 9 applies. The exemptions include, for example, the situation where processing is necessary for reasons of substantial public interest. Schedule 1 to the Bill provides a series of processing conditions for special categories of data under article 9 and criminal convictions data under article 10. Most of those processing conditions have been imported from the Data Protection Act 1998 and statutory instruments made under that Act, but some of them are new—for example, the conditions on anti-doping...
in sport or processing for insurance purposes. They have been added to reflect the way in which the use of data has changed over the past 20 years.

Amendment 129 would remove the ability to amend schedule 1 via secondary legislation. That would be particularly damaging because it would mean that primary legislation might be needed every time for a new processing activity involving special categories of data arose. The 1998 Act was itself amended several times through secondary legislation, and it is important that we retain the flexibility to respond to emerging technologies and the different ways in which data might be used in the future.

It is interesting to note that the hon. Member for Sheffield, Heeley has tabled an amendment to schedule 1 that would add a completely new processing condition in relation to maintaining the missing persons register. My hon. Friend the Under-Secretary of State for the Home Department will touch on the merits of that proposal later, but the fact that others in the Committee are considering further changes to schedule 1 illustrates the point that schedule 1 cannot simply freeze the regimes in parts 3 and 4 of the Bill. I urge colleagues to resist the amendment.

Stuart C. McDonald: It is vital that we get the balance right: we are talking about very sensitive information and processing of that information. It is absolutely right for hon. Members to table amendments to the Bill and for them to be considered, including proposals on the missing persons register. The fact that hon. Members are suggesting changes at this stage does not mean that we are saying that we want to fix things for all time now and never suggest changes again. We are saying that we are not happy with the process whereby changes are brought about. The Minister has not explained why she believes that changes could not be brought about satisfactorily by changes to legislation from time to time. She has not explained why there would be urgent situations in which the only possibility would be a “Take it or leave it” statutory instrument. In the light of the seriousness of the data that we are speaking about and the inadequacy of the Minister’s explanation, we would like to press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 9, Noes 10.

Division No. 2]

AYES

Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren
McDonald, Stuart C.

Murray, Ian
O’Hara, Brendan
Snell, Gareth
Zeichner, Daniel

NOES

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

James, Margot
Lopez, Julia
Warman, Matt
Wood, Mike

Question accordingly negatived.

Clause 10 ordered to stand part of the Bill.

Schedule 1

SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL CONVICTIONS ETC DATA

Margot James: I beg to move amendment 76, in schedule 1, page 123, line 21, at beginning insert “Except as otherwise provided.”.

This amendment is consequential on Amendments 79, 82 and 90.

The Chair: With this it will be convenient to discuss Government amendments 77 to 83 and 87 to 91.

Margot James: Part 2 of schedule 1 sets out a series of processing activities that are considered to be or have the potential to be in the substantial public interest. That is important in ensuring that such activities can continue even in the absence of explicit consent and even where they require special categories of personal data to be processed.

I am pleased to introduce amendment 78 today. It will help businesses and other organisations ensure that boardrooms and senior management levels are truly representative of the workforce they manage and the communities they serve. In my former role at the Department for Business, Energy and Industrial Strategy, I worked closely with Sir John Parker, to whom I pay great tribute for the work that he has done in this area. I worked with him to examine how we could ensure that more FTSE 100 companies and others did more to attract talent from a wide range of racial and ethnic backgrounds.

In November 2016, Sir John published a report that showed that although 14% of the population identified as black, Asian or other minority ethnic status, only 1.5% of directors in FTSE 100 boardrooms were UK citizens from such a minority. Although significant progress has been made in recent years to improve the gender balance in the boardrooms of such companies, the severe under-representation of people from minority ethnic backgrounds cannot be tolerated in modern society. Sir John’s report included a series of recommendations to improve ethnic diversity in the boardroom. He encouraged companies to make better use of executive search firms to identify potential candidates and invite them to be interviewed for managerial vacancies.

Amendment 78 will add a new processing condition to schedule 1 to allow organisations to process personal data about potential candidates’ racial or ethnic origin and identify suitable candidates for potential board or managerial positions. The processing condition will apply only until such point as it is reasonable to expect the organisation to get the potential candidate’s consent to the continued processing of their racial and ethnic origin data. If the data subject gave a positive indication that she or he did not consent to the processing of such data, the controller would have to cease processing the data.

I hope that hon. Members welcome the steps we are taking to implement the recommendations of the Parker review. We believe that it is in the interest of society as a whole to ensure that businesses and other organisations recruit the best person for the job if they are going to compete in today’s economy. People from all backgrounds should be given equal opportunities to contribute.
11.15 am

I am also pleased to introduce amendment 83, concerning patient support, which honours a commitment made by the Government to my noble Friend, Baroness Neville-Jones during the Bill's passage through the Lords. She spoke passionately on behalf of the patient support group Unique, which maintains a register of patients suffering from very rare and sometimes life-limiting chromosomal disorders. Over the years, it has built up a database of around 18,000 patients, which it uses to provide invaluable guidance and support to new and existing members, who may not know what to expect from the different stages of a particular disorder. It even uses the database to advise GPs and other medical professionals about probable symptoms so that they can help patients at the time of diagnosis. Amendment 83 adds a new processing condition to the schedule to provide Unique and groups like it with the legal certainty they require to continue their vital work.

During the Lords stages of the Bill, Thomson Reuters provided their lordships with a helpful briefing note setting out how it compiles reports on persons suspected of terrorism, bribery, money laundering, modern slavery and other reprehensible activities. It shares that information with banks to help them avoid mixing with such people and to allow them to comply with their regulatory obligations and other internationally recognised guidelines. In response to support for the proposal on both sides of the House of Lords, the Government committed to working with Thomson Reuters to bring forward amendments at a later stage of the Bill's passage.

Amendment 81 is the culmination of that work. It adds a new processing condition to the schedule to allow organisations such as Thomson Reuters, and banks themselves, to screen customers and suppliers for criminal activities and other seriously improper conduct. The condition can be used only in circumstances where the controller cannot reasonably be expected to obtain the data subject's consent to process data—for example, where the controller processes data from sanction lists and other seriously improper conduct. It allows making it more difficult for offenders to launder the proceeds of their crime. I am grateful for the help that Thomson Reuters provided my officials with developing the provision.

Moving to the technical amendments in the group, amendment 88 corrects a mistake in the drafting of paragraph 16 of the schedule relating to processing in connection with occupational pensions.

Liam Byrne: Oh dear!

Margot James: It does happen. That is not a new provision, but one that was imported from the current law. Unfortunately, some crucial words were accidentally lost in the process of importing it. The amendment reinstates them.

Schedule 1 sets out UK domestic legislation to allow the processing of particularly sensitive data in certain circumstances. The Government's view is that the processing of such data must be undertaken with adequate and appropriate safeguards to ensure that individuals' most sensitive data is appropriately protected. One of those safeguards is the new requirement for an appropriate policy document to be maintained in most circumstances when special categories of data and criminal convictions data are processed. That is set out in paragraph 5 and part 4 of the schedule.

Since the Bill's introduction, we have reflected on whether there are cases where the requirement to hold an appropriate policy document is so disproportionate that, rather than improving protections, it effectively prevents the necessary processing from taking place. Amendments 79, 82 and 90 remove the requirement for a controller to have an appropriate policy document where processing involves the disclosure of special category data to a competent authority for the detection or prevention of an unlawful act, the disclosure of special category data for specific purposes in connection with journalism, or the disclosure of special category data to an anti-doping authority. Amendment 80 defines what is meant by "competent authority". The aim of those amendments is to avoid a scenario in which an individual who never normally processes data under schedule 1 wishes to report a crime, report something of public interest to the media or report doping activities in sport and, in so doing, processes special categories of data and would have to have in place an appropriate policy document.

Amendment 76 reflects that change to the requirement to have an appropriate policy document by inserting the words, “Except as otherwise provided” in paragraph 5 of the schedule. Amendments 87 and 89 make it clear that, in the context of schedule 1, “withholding consent” means doing something purposeful, not just neglecting to reply to a letter from the data controller. That avoids a world in which data controllers have an incentive not to bother requesting consent in the first place.

Paragraph 31 of the schedule requires the controller to have an appropriate policy document in place when relying on a processing condition in part 2 of the schedule to process criminal convictions data. However, all the provisions in part 2 are subject to the policy document requirement except where noted, so there is no reason to state it again in paragraph 31. Amendment 91 removes that duplicate requirement. It is simply a tidying-up amendment to improve the coherence of the Bill.

Darren Jones: On a point of order, Mr Hanson. I think I was remiss in not declaring my interest at the start of my contributions to today's proceedings. With your permission, I seek to rectify that.

The Chair: That is indeed a point of order. The record will show that the hon. Gentleman has now declared his interest in relation to his contributions to the debate.

Ordered, That the debate be now adjourned.—(Nigel Adams.)

11.22 am

Adjourned till this day at Two o'clock.
Public Bill Committee

DATA PROTECTION BILL [LORDS]

Second Sitting
Tuesday 13 March 2018
(Afternoon)

CONTENTS

Schedule 1 agreed to, with amendments.
Clauses 11 to 15 agreed to, some with amendments.
Schedules 2 to 4 agreed to, some with amendments.
Clauses 16 and 17 agreed to, one with an amendment.
Schedule 5 agreed to, with an amendment.
Clauses 18 to 22 agreed to, one with an amendment.
Adjourned till Thursday 15 March at half-past Eleven o’clock.
Written evidence reported to the House.
No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Saturday 17 March 2018

© Parliamentary Copyright House of Commons 2018

This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright/.
The Committee consisted of the following Members:

**Chairs:** †David Hanson, Mr Gary Streeter

† Adams, Nigel (*Lord Commissioner of Her Majesty’s Treasury*)
† Atkins, Victoria (*Parliamentary Under-Secretary of State for the Home Department*)
† Byrne, Liam (*Birmingham, Hodge Hill*) (Lab)
† Clark, Colin (*Gordon*) (Con)
† Elmore, Chris (*Ogmore*) (Lab)
† Haigh, Louise (*Sheffield, Heeley*) (Lab)
† Heaton-Jones, Peter (*North Devon*) (Con)
† Huddleston, Nigel (*Mid Worcestershire*) (Con)
† Jack, Mr Alister (*Dumfries and Galloway*) (Con)
† James, Margot (*Minister of State, Department for Digital, Culture, Media and Sport*)
† Jones, Darren (*Bristol North West*) (Lab)
† Lopez, Julia (*Hornchurch and Upminster*) (Con)
† McDonald, Stuart C. (*Cumbernauld, Kilsyth and Kirkintilloch East*) (SNP)
† Murray, Ian (*Edinburgh South*) (Lab)
† O’Hara, Brendan (*Argyll and Bute*) (SNP)
† Snell, Gareth (*Stoke-on-Trent Central*) (Lab/Co-op)
† Warman, Matt (*Boston and Skegness*) (Con)
† Wood, Mike (*Dudley South*) (Con)
† Zeichner, Daniel (*Cambridge*) (Lab)

Kenneth Fox, Committee Clerk

† attended the Committee
Amendment proposed (this day): 76, in schedule 1, page 123, line 21, at beginning insert “Except as otherwise provided.”

This amendment is consequential on Amendments 79, 82 and 90. —(Margot James.)

2 pm Question again proposed. That the amendment be made.

The Chair: I remind the Committee that with this we are discussing Government amendments 77 to 83 and 87 to 91.

Amendment 76 agreed to.

Amendments made: 77, in schedule 1, page 124, line 24, leave out from “subject” to end of line 25.

In paragraph 8 of Schedule 1, sub-paragraph (3) contains an exception from the condition in sub-paragraph (1). This amendment would remove from the exception the requirement that the processing is carried out without the data subject’s consent.

Amendment 78, in schedule 1, page 124, line 36, at end insert—

“Racial and ethnic diversity at senior levels of organisations

8A (1) This condition is met if the processing—

(a) is of personal data revealing racial or ethnic origin,
(b) is carried out as part of a process of identifying suitable individuals to hold senior positions in a particular organisation, a type of organisation or organisations generally,
(c) is necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation or organisations, and
(d) can reasonably be carried out without the consent of the data subject,

subject to the exception in sub-paragraph (3).

(2) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and
(b) the controller is not aware of the data subject withholding consent.

(3) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(4) For the purposes of this paragraph, an individual holds a senior position in an organisation if the individual—

(a) holds a position listed in sub-paragraph (5), or
(b) does not hold such a position but is a senior manager of the organisation.

(5) Those positions are—

(a) a director, secretary or other similar officer of a body corporate;
(b) a member of a limited liability partnership;
(c) a partner in a partnership within the Partnership Act 1890, a limited partnership registered under the Limited Partnerships Act 1907 or an entity of a similar character formed under the law of a country or territory outside the United Kingdom.

(6) In this paragraph, “senior manager”, in relation to an organisation, means a person who plays a significant role in—

(a) the making of decisions about how the whole or a substantial part of the organisation’s activities are to be managed or organised, or
(b) the actual managing or organising of the whole or a substantial part of those activities.

(7) The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.”.

Part 2 of Schedule 1 describes types of processing of special categories of personal data which meet the requirement in Article 9(2)(g) of the GDPR (processing necessary for reasons of substantial public interest) for a basis in UK law (see Clause 10(3)). This amendment adds to Part 2 of Schedule 1 certain processing of personal data for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in organisations.

Amendment 79, in schedule 1, page 125, line 3, at end insert—

“( ) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).”.

This amendment, and Amendment 80, provide that where processing falling within paragraph 9 of Part 2 of Schedule 1 (preventing or detecting unlawful acts) consists of, or is carried out in preparation for, the disclosure of personal data to a competent authority, the condition in that paragraph is met even if the controller does not have an appropriate policy document in place when the processing is carried out.

Amendment 80, in schedule 1, page 125, line 4, at end insert—

“( ) “competent authority” has the same meaning as in Part 3 of this Act (see section30).”.

See the explanatory statement for Amendment 79.

Amendment 81, in schedule 1, page 125, line 16, at end insert—

“Regulatory requirements relating to unlawful acts and dishonesty etc

10A (1) This condition is met if—

(a) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has—

(i) committed an unlawful act, or
(ii) been involved in dishonesty, malpractice or other seriously improper conduct,

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and
(c) the processing is necessary for reasons of substantial public interest.

(2) In this paragraph—

“act” includes a failure to act;
“regulatory requirement” means—
(a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or
(b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.”.

Part 2 of Schedule 1 describes types of processing of special categories of personal data which meet the requirement in Article 9(2)(g) of the GDPR (processing necessary for reasons of substantial public interest) for a basis in UK law (see Clause 10(3)). This amendment adds to Part 2 of Schedule 1 certain processing of personal data for the purposes of complying with, or assisting others to comply with, a regulatory requirement.

Amendment 82, in schedule 1, page 125, line 35, at end insert—

“( ) The condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).”.

This amendment provides that the condition in paragraph 11 of Part 2 of Schedule 1 (journalism etc in connection with unlawful acts and dishonesty etc) is met even if the controller does not have an appropriate policy document in place when the processing is carried out.

Amendment 83, in schedule 1, page 126, line 22, at end insert—

“Support for individuals with a particular disability or medical condition

13A (1) This condition is met if the processing—
(a) is carried out by a not-for-profit body which provides support to individuals with a particular disability or medical condition,
(b) is of a type of personal data falling within sub-paragraph (2) which relates to an individual falling within sub-paragraph (3),
(c) is necessary for the purposes of—
(i) raising awareness of the disability or medical condition, or
(ii) providing support to individuals falling within sub-paragraph (3) or enabling such individuals to provide support to each other;
(d) can reasonably be carried out without the consent of the data subject, and
(e) is necessary for reasons of substantial public interest.

(2) The following types of personal data fall within this sub-paragraph—
(a) personal data revealing racial or ethnic origin;
(b) genetic data or biometric data;
(c) data concerning health;
(d) personal data concerning an individual’s sex life or sexual orientation.

(3) An individual falls within this sub-paragraph if the individual is or has been a member of the body mentioned in sub-paragraph (1)(a) and—
(a) has the disability or condition mentioned there, has had that disability or condition or has a significant risk of developing that disability or condition, or
(b) is a relative or carer of an individual who satisfies paragraph (a) of this sub-paragraph.

(4) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—
(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and
(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph—
“carer” means an individual who provides or intends to provide care for another individual other than—
(a) under or by virtue of a contract, or
(b) as voluntary work;
“disability” has the same meaning as in the Equality Act 2010 (see section 6 of, and Schedule 1 to, that Act).

(6) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.”.—(Margot James.)

Part 2 of Schedule 1 describes types of processing of special categories of personal data which meet the requirement in Article 9(2)(g) of the GDPR (processing necessary for reasons of substantial public interest) for a basis in UK law (see Clause 10(3)). This amendment adds to Part 2 of Schedule 1 certain processing of personal data by not-for-profit bodies involved in supporting individuals with a particular disability or medical condition.

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): I beg to move amendment 84, in schedule 1, page 126, line 27, leave out “a reason” and insert “one of the reasons”. This amendment amends paragraph 14(1)(b) of Schedule 1 for consistency with paragraphs 18(2) and 19(2) of that Schedule.

The Chair: With this it will be convenient to discuss Government amendments 85, 86, 116 and 117.

Victoria Atkins: It is a pleasure to serve under your chairmanship, Mr Hanson. I am pleased to introduce this group of amendments, which relate to data processing for safeguarding purposes. The amendments respond to an issue raised in an amendment tabled by Lord Stevenson on Report in the Lords in December. In response to that amendment, Lord Ashton made it clear that the Government are sympathetic to the points Lord Stevenson raised and undertook to consider the matter further. Amendments 85, 116 and 117 are the result of that consideration.

I am grateful to Lord Stevenson for raising this issue, and for his contribution to what is probably the most important new measure that we intend to introduce to the Data Protection Bill. The amendments will ensure that sensitive data can be processed without consent in certain circumstances for legitimate safeguarding activities that are in the substantial public interest. We have been working across government and with stakeholders in the voluntary and private sectors to ensure that the amendments are fit for purpose and cover the safeguarding activities expected of organisations responsible for children and vulnerable adults.

The Government recognise that statutory guidance and regulator expectations place moral, if not legal, obligations on certain organisations to ensure that measures are in place to safeguard children and vulnerable adults. Amendment 85 covers processing that is necessary for protecting children and vulnerable adults from neglect or physical or mental harm. This addresses the gap in relation to expectations on, for example, sports governing bodies.

The Government have produced cross-agency and cross-governmental guidance called “Working Together to Safeguard Children”, which rightly places the responsibility of safeguarding children on all relevant professionals who come into contact with children and families. For example, it creates an expectation that those volunteering at a local sports club will assess the needs of children and, importantly, will take action to protect them from abuse.

Amendment 85 permits the processing of sensitive personal data, which is necessary to safeguard children from physical, emotional, sexual and neglect-based abuse.
Amendment 84 makes a consequential drafting change, while amendments 116 and 117 make an analogous change to the regimes in parts 3 and 4 of the Bill. This is aimed at putting beyond doubt a controller’s ability to safeguard children and people at risk.

I thought an example might help the Committee to understand why we place such an emphasis on the amendments. An example provided by a sports governing body is that a person may make an allegation or complaint about a volunteer that prompts an investigation. Such investigations can include witness statements, which reference sensitive personal data, including ethnicity, religious or philosophical beliefs, sexual orientation and health data.

In some instances, the incident may not reach a criminal standard. In those cases, the sports body may have no legal basis for keeping the data. Keeping a record allows sports bodies to monitor any escalation in conduct and to respond appropriately. Forcing an organisation to delete this data from its records could allow individuals that we would expect to be kept away from children to remain under the radar and potentially leave children at risk.

Amendment 86 deals with a related issue where processing health data is necessary to protect an individual’s economic wellbeing, where that individual has been identified as an individual at economic risk. UK banks have a number of regulatory obligations and expectations which are set out in the Financial Conduct Authority’s rules and guidance. In order to meet best practice standards in relation to safeguarding vulnerable customers, banks occasionally need to record health data without the consent of the data subject.

An example was given of a bank which was contacted by a family member who was alerting the bank to an elderly customer suffering from mental health problems who was drawing large sums of money each day from their bank account and giving it away to a young drug addict whom they had befriended. The bank blocked the account while the family sought power of attorney. Again, the amendment seeks to clarify the position and give legal certainty to banks and other organisations where that sort of scenario arises or where, for example, someone suffers from dementia and family members ask banks to take steps to protect that person’s financial wellbeing.

The unfortunate reality is that there still exists a great deal of uncertainty under current law about what personal data can be processed for safeguarding purposes. My brief of crime, vulnerability and safeguarding means that all too often—perhaps in the context of domestic abuse—agencies will gather, sadly, to conduct a domestic homicide review and discover that had certain pieces of information been shared more freely, perhaps more action could have been taken by the various agencies and adults and children could have been safeguarded.

These amendments are aimed at tackling these issues. We want to stop the practice whereby some organisations have withheld information from the police and other law enforcement agencies for fear of breaching data protection law and other organisations have been unclear as to whether consent to processing personal data is required in circumstances where consent would not be reasonable or appropriate. The amendments intend to address the uncertainty by providing relevant organisations with a specific processing condition for processing sensitive personal data for safeguarding purposes. I beg to move.

Liam Byrne (Birmingham, Hodge Hill) (Lab): I rise to put on record my thanks to the Minister for listening carefully to my noble Friend Lord Stevenson. There was strong cross-party consensus on these common-sense reforms.

We all know that in our own constituencies there are extraordinary people doing extraordinary things in local groups. They are the life-blood of our communities. Many of them will be worried about the new obligations that come with the general data protection regulation and many of them will take a least-risk approach to meeting the new regulations. Putting in place some common safeguards to ensure that it is possible to keep data that allow us to spot important patterns of behaviour that can lead to appropriate investigations is very sensible and wise. These amendments will therefore be made with cross-party support.

Amendment 84 agreed to.

Amendments made: 85, page 126, line 38 [Schedule 1], at end insert—

“Safeguarding of children and of individuals at risk

14A (1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is “at risk” if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.”
Amendment 86, page 126, line 38 [Schedule 1], at end insert—

“Safeguarding of economic well-being of certain individuals

14B (1) This condition is met if the processing—

(a) is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 or over,
(b) is of data concerning health,
(c) is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and
(d) is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;
(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;
(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) In this paragraph, “individual at economic risk” means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability.”—[(Victoria Atkins.)]

Part 2 of Schedule 1 describes types of processing of special categories of personal data which meet the requirement in Article 9(2)(g) of the GDPR (processing necessary for reasons of substantial public interest) for a basis in UK law (see Clause 10(3)). This amendment adds to Part 2 of Schedule 1 certain processing of personal data which is necessary to protect the economic well-being of adults who are less able to protect their economic well-being by reason of a physical or mental injury, illness or disability.

Louise Haigh (Sheffield, Heeley) (Lab): I beg to move amendment 150, page 126, line 38, at end insert—

“Register of missing persons

14A This condition is met if the processing—

(a) is necessary for the establishment or maintenance of any register of missing persons, and
(b) is carried out in a manner which is consistent with any guidance which may be issued by the Secretary of State or by the Commissioner on the processing of data for the purposes of this paragraph.”

It is a pleasure to serve under your chairmanship, Mr Hanson. Amendment 150 seeks to provide a similar exemption to the one that the Minister has just laid out. As my right hon. Friend the Member for Birmingham, Hodge Hill said, we completely support the principles behind this exemption to schedule 1. As the Minister made clear, too often serious case reviews or reviews after an incident of this nature, particularly in child protection cases, show clearly that if the data had been shared more effectively—often in health cases—the child could have been protected and their life might have been saved.

We tabled this amendment because of the increase in the number of missing persons and missing children over the past few years. As the shadow Police Minister, I approach this issue from a policing perspective. It is important that all data handlers fully understand their obligations and the powers that are bestowed on them. Too often, under the existing legislation, they hide behind data protection to avoid sharing data, and we fear that that tendency will become even stronger under the Bill.

Sharing data relating to missing persons is important for a number of reasons. The demand on police services from such cases has rocketed over the past few years. Police officers spend only 17% of their time responding to crime, so 83% of police time is spent responding to non-crime demand. That includes mental health call-outs, but largely it relates to missing persons. Some police forces tell me that missing persons place the greatest demand on their time.

In the west midlands, since 2015 the number of missing person incidents has doubled to nearly 13,000 cases a year. In Northumbria—one of the smallest police forces in the country—as of this minute there are 43 men and 20 women missing. For such a small police force, that is a significant number of people to be out looking for. Last year alone, such investigations cost the police service more than £600 million. One fifth of those missing persons are children in care, more than 50% are children, and a significant proportion are elderly people missing from care. Crucially, about one third are reported missing on more than one occasion. It is those individuals we seek to address with the register.

There are various reasons for the increase, one of which is certainly better police reporting. Our ageing population means that more people are in care and are going missing from care. The police have responded to that issue in various ways, including by tagging elderly individuals who go missing from care repeatedly—we have tabled amendments to explore the issues arising from that. Cuts to other public services mean that the increasing demand, which previously would have fallen elsewhere—in particular, on local authorities—is now landing on the police. We are seeing a higher tolerance of risk across the care sector, and possibly the health sector too, and a tendency to pass the buck for these issues and other vulnerabilities on to the police, who have a very low risk threshold and nowhere to pass them on.

I believe we need a review of all agencies that are involved with safeguarding to ensure that they are taking seriously their responsibilities in this regard. When the issue relates to resources, they must make the case for those resources, rather than merely pass the problem on to the police. I have heard stories about private children’s care homes where staff may see that the child is outside their window or down the street, but because they are five minutes over curfew they ring the police and say that the child is missing. That messes with the responsibilities, but has very serious implications for the police. It diverts resources from tackling crime and from responding to genuine cases of missing children and high-risk missing persons.

Estimates of the time associated with this activity suggest that approximately 18 hours of police time is needed for a medium-risk missing persons investigation. In 2015-16, that equated to more than 6 million investigation hours, or more than 150,000 officers occupied full time with that activity. Not being dealt with by the appropriate agency and not being responded to correctly has real implications for the individual. Going missing can be a precursor to various aspects of significant harm, such as abuse, exposure to criminal activity and mental ill-health. There are enough issues relating to police forces sharing data among themselves, let alone with other agencies. As a result, various criminal activities exploiting those weaknesses have developed. In the past, the Minister and I have discussed county lines at length, which is a criminal activity whereby organised criminal gangs exploit children. They take them, internally traffic them across the country, set them up in another vulnerable adult’s
home and leave them to deal drugs on their behalf. That is a very profitable criminal activity, but the perpetrators have been able to evade real enforcement because of the weaknesses in data sharing and cross-agency working between police forces and agencies. The amendment will ensure that the police and all appropriate safeguarding agencies have access to the relevant data to ensure that at-risk missing people are found as quickly and safely as possible, and have their needs dealt with in the most appropriate way.

2.15 pm

I know that the Government are supportive of that idea and proposal. In their “Tackling child sexual exploitation: progress report” they recognise the need to improve the early identification of and initial response to children and young people at risk. They have committed to extend their programme of work into child safeguarding, and a key deliverable was the development of a national missing persons register. This amendment seeks to probe the Government about the establishment of that register, and about the information that it should include.

We believe—the Children’s Society has made representations on this—that if designed well, key information and intelligence could be stored in one place, making the sharing of vital information about missing people in real time possible across different local areas. The information available should include previously identified risks, where people go missing from and to, and who they go missing with. Furthermore, the register should include provision for local authorities or return-home interview service providers commissioned by local authorities to input and store relevant information from those interviews, to inform risk assessment and local intelligence on missing children.

In 2016, Her Majesty’s Inspectorate of Constabulary found serious inconsistencies between and within forces regarding data sharing and responding to missing children and high-risk missing adults. This issue has been highlighted by the inspectorate, and I am sure that the Minister understands the urgency of getting such a register in place. The case for the amendment is clear: it supports the principles that have been outlined by the Government, and it would support our most vulnerable people and go some way towards relieving pressure on the police when responding to those high-risk missing people.

Victoria Atkins: I am grateful to the hon. Member for Sheffield, Heeley for affording me the opportunity to update the Committee on our progress in establishing a national register of missing persons, and to touch on the missing children and adults strategy that the Government are currently working on, which I hope will be published shortly. It will address many of the themes that the hon. Lady drew on in her speech, particularly the deliberate targeting of vulnerable children by county lines gangs, children who go missing—usually, sadly, from care homes—and the exploitation that occurs.

As the hon. Lady said, this is an important subject because each year more than 337,000 calls are made to police stations identified and Whitehall concerns identified about missing and absent people. Happily, the vast majority are found within 24 hours, but 2% or thereabouts remain missing for more than a week. Anyone who has ever met the parents of children who go missing knows the heartache that those parents face, not just on an annual basis, but on a daily, minute-by-minute basis. They feel that pain constantly.

People who go missing are often the most vulnerable in society, and it is vital that those tasked with investigating their disappearance have the most accurate and up-to-date information available. We accept that the current technology available to frontline staff to deal with missing persons is insufficient. For example, the police national computer identifies only those currently reported as missing, while the National Crime Agency database includes only those missing for more than 72 hours. We know that the search must start the moment that a child or vulnerable person is identified as missing; we cannot wait for 72 hours. There is no national record of the history of missing persons in England and Wales.

The Government’s “Tackling child sexual exploitation: progress report” published in February last year set out our commitment to deliver a national missing persons register. This will enable police officers to access up-to-date data about missing people across force boundaries and take appropriate action when they investigate missing person incidents or encounter a missing person who is away from his or her home force area. The register is being established as part of the national law enforcement data programme, which will replace the police national computer and the police national database with a new national data service. The current timetable, agreed with the police, is to launch the capability for forces to record manually missing and associated found incidents from mid-2019 with releases thereafter, including automation and establishing the ability to share controlled information beyond policing to other agencies.

In terms of the way in which the register and the scheme interplay in the Bill, the processing of the personal data held on the database will take place under either the GDPR or part 3 of the Bill. Processing of the data by the police will often be for a law enforcement purpose, including the prevention, investigation or detection of a criminal offence and any sensitive processing would fall within paragraph 3 of schedule 8, which enables processing where necessary to protect the vital interests of the data subject or another individual, or under the new safeguarding condition, which we have just debated. Where the processing is undertaken under the GDPR, the conditions in respect of protecting the vital interests of the data subject, or preventing or detecting unlawful acts, may apply. Again, the new safeguarding condition may also be applicable.

Given those provisions and the very clear timetable that the Government and police have for their programme, we are of the view that the amendment is unnecessary, but I am, of course, very appreciative that the hon. Lady has raised this in the Committee. Obviously, I will keep her informed of progress on the new register.

Louise Haigh: That is fantastic news. It is a very ambitious deadline for a police IT transformation programme. I know that South Yorkshire is going through the transformation on the CONNECT programme at the moment; it is woefully behind the timescale envisaged and over budget, as every IT transformation in the history of any Government, of any colour, has always been. I wonder, therefore, given the urgency of this issue, whether it is possible for this information to be recorded on the PNC for the time being.
Victoria Atkins: I am looking at my officials and they will stop me if I am wrong. I hope. If she prefers, may I write to her? I do not think that the PNC has the capability at the moment. That is why we are having to develop this new programme, but we will write to the hon. Lady in any event. As I say, I will keep her up-to-date with progress. But I invite her to withdraw the amendment, please.

Louise Haigh: Given that the Minister asked so nicely, I will. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Amendments made: 87, in schedule 1, page 127, line 30, at end insert—

“( ) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.”

This amendment clarifies the intended effect of the safeguard in paragraph 15(4) of Schedule 1 (processing necessary for an insurance purpose).

Amendment 88, in schedule 1, page 127, line 39, at end insert—

“( ) is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme.”

This amendment provides that the condition in paragraph 16 of Schedule 1 (occupational pension schemes) can only be relied on in connection with the processing of data concerning health relating to certain relatives of a member of the scheme.

Amendment 89, in schedule 1, page 128, line 6, at end insert—

“( ) The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.”

This amendment clarifies the intended effect of the safeguard in paragraph 16(2) of Schedule 1 (processing necessary for determinations in connection with occupational pension schemes).

Amendment 90, in schedule 1, page 131, line 14, at end insert—

“( ) If the processing consists of the disclosure of personal data to a body or association described in sub-paragraph (1)(a), or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).”

This amendment provides that when processing consists of the disclosure of personal data to a body or association that is responsible for eliminating doping in sport, or is carried out in preparation for such disclosure, the condition in paragraph 22 of Part 2 of Schedule 1 (anti-doping in sport) is met even if the controller does not have an appropriate policy document in place when the processing is carried out.

Amendment 91, in schedule 1, page 133, line 17, leave out from “interest” to end of line 21.—( ) (Margot James.)

This amendment removes provisions from paragraph 31 of Schedule 1 (extension of conditions in Part 2 of Schedule 1 referring to substantial public interest) which are unnecessary because they impose requirements which are already imposed by paragraph 5 of Schedule 1.

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): I beg to move amendment 92, page 134, line 18 [Schedule 1], leave out “on the day” and insert “when”.

This amendment is consequential on Amendment 71.

The Chair: With this it will be convenient to discuss the following:

Government amendments 107, 108, 111, 113, 114, 21, 29 to 40, 43 to 46, 118 to 121, 48, 49, 53, 55, 56, 123 to 125, 59 and 71.

Margot James: Following engagement with local government stakeholders, we have recognised that the maximum time period permitted for responses to the subject access request set out in parts 3 and 4 of the Data Protection Bill subtly differs from that permitted under the GDPR and part 2 of the Bill. That is because the GDPR and, by extension, part 2 rely on European rules for calculating time periods, whereas parts 3 and 4 implicitly rely on a more usual domestic approach. European law, which applies to requests under part 2, says that when one is considering a time period in days, the day on which the request is received is discounted from the calculation of that time period. In contrast, the usual position under UK law, which applies to requests under parts 3 and 4 of the Bill, is that the same seven-day period to respond would begin on the day on which the request was received. In a data protection context, that has the effect of providing those controllers responding to requests under parts 3 and 4 with a time period that is one day shorter in which to respond.

To provide consistency across the Bill, we have decided to include a Bill-wide provision that applies the European approach to all time periods throughout the Bill, thus ensuring consistency with the directly applicable GDPR. Having a uniform approach to time periods is particularly helpful for bodies with law enforcement functions, which will process personal data under different regimes under the Bill. Without these amendments, different time periods would apply, depending on which regime they were processing under. Ensuring consistency for calculating time periods will also assist the information commissioner with her investigatory activities and enforcement powers, for example by avoiding the confusion and potential disputes that could arise relating to her notices or requests for information.

Amendment 71 provides for a number of exemptions to the European approach where deviating from our standard approach to time periods would be inappropriate. For example, where the time period refers to the process of parliamentary approval of secondary legislation, it would clearly not be appropriate to deviate from usual parliamentary time periods. The unfortunate number of amendments in this group comes from the need to modify existing language on time periods that are currently worded for compliance with the usual UK approach, whereas parts 3 and 4 implicitly rely on a more usual domestic approach. European law, which applies to requests under part 2, says that when one is considering a time period in days, the day on which the request is received is discounted from the calculation of that time period. In contrast, the usual position under UK law, which applies to requests under parts 3 and 4 of the Bill, is that the same seven-day period to respond would begin on the day on which the request was received. In a data protection context, that has the effect of providing those controllers responding to requests under parts 3 and 4 with a time period that is one day shorter in which to respond.

Amendment 92 agreed to.

Question proposed. That the schedule, as amended, be the First schedule to the Bill.

Liam Byrne: We had a useful debate this morning about the whys and wherefores of whether the article 8 right to privacy should be incorporated into the Bill. Although we were disappointed by the Minister's reply, what I thought was useful in the remarks she made was a general appreciation of the importance of strong data rights if the UK is to become a country with a strong environment of trust within which a world of digital trade can flourish.

I will briefly alert the Minister to a debate we want to have on Report. The reality is that we feel schedule 1 is
narrowly drawn. It is an opportunity that has been missed, and it is an opportunity for the Minister to come back on Report with a much more ambitious set of data rights for what will be a digital century. When we look around the world at the most advanced digital societies, we can see that a strong regime of data rights is common to them all.

I was recently in Estonia, which I hope the Minister will have a chance to visit if she has not done so already. Estonia likes to boast of its record as the world’s most advanced digital society; it is a place where 99% of prescriptions are issued online, 95% of taxes are paid online and indeed a third of votes are cast online. It is a country where the free and open right to internet access is seen as an important social good, and a good example of a country that has really embraced the digital revolution and translated that ambition into a set of strong rights.

The Government are not averse to signing declaratory statements of rights that they then interpret into law. They are a signatory to the UN universal declaration of human rights and the UN convention on the rights of the child; the Human Rights Act 1998 is still in force—I have not yet heard of plans to repeal it—and of course the Equality Act 2010 was passed with cross-party support. However, those old statements of rights, which date back to 1215 and the worries that the barons had about King John. We are no longer as concerned as people were in 1215 about taking all the fish weirs out of the Thames, for example.

2.30 pm

The reality today is that we are not worried about the unchecked powers of sovereigns, but we are more and more concerned about the power of big tech companies. As of last Friday, the fearsome five data giants had a combined market capitalisation of about $2.4 trillion. They are very, very powerful players. They capture data from us and process it in a way that we do not really understand, with effects that we do not really appreciate. The Government have nodded towards that concern with the idea of setting up a digital charter, which is very much from the cones hotline school of public service reform. The problem with a digital charter is that it will contain vague commitments associated with vague frameworks, without much legislative bite. We think the Government can do much better.

Of course, that is brought into focus most sharply with regard to children. Children are not a marginal issue in this debate; they are about a third of internet users. We were grateful that the Government acquiesced in amendments moved by Baroness Kidron. She is one of the architects of the 5Rights movement, which says that children should have the right to remove content they do not want to be online anymore; the right to know who is targeting them and for what purposes; the right to safety and support, because children are often upset or abused online; the right to informed and conscious use; and the right to digital literacy. The 5Rights movement has helped set out those good, strong digital rights for children, but we urge the Government to build on the basic charter of digital rights in schedule 1 and go much further.

The amendments we tabled that were not selected for debate—we hope we will be able to come back to them at a later stage—include the following. One relates to the right to equality of access: every data subject should have the right to access and participate in the digital environment on equal terms, and internet access should be open and free. Another is about equality of treatment: every data subject should have the right to fair and equal treatment in the processing of his or her personal data, in a way that is encompassed by many amendments to the Bill. A third relates to security: every data subject should have the right to security and protection of their personal data and information systems, and Governments should not misuse their ability to access that information without checks and safeguards.

There should be rights to free expression through data, to privacy and to ownership of data. Every data subject should have the right to own and control their personal data and therefore should be entitled to a proportionate share of the income or other benefit derived from it. Every data subject should have the right to transparent and equal treatment in the processing of their personal data by an algorithm or an automated system. Every data subject should have the right to deploy their personal data to communicate, in pursuit of their fundamental right to freedom of association. There should be strong rights to protection online, and to remove data.

We think that a more ambitious and assertive schedule 1 could be the foundation of a strong digital Bill of Rights for the 21st century, which would go some way to creating a stronger environment of trust online. Trust is breaking down, because cyber-crime is multiplying, because public services such as the NHS have shown their vulnerability to cyber-attacks and because of the proliferation of fake news. There is wide appreciation that our children in particular are vulnerable, and I am afraid there is concern that the Government have been too reluctant to act.

Although the digital charter takes the debate on somewhat, we would encourage the Government, in the best traditions of this country and in the best tradition of our contribution to the debate about strong rights, to be more assertive and more ambitious in schedule 1 and to accommodate the amendments we will table on Report.

The Chair: To make matters clear to hon. Members and in particular who are new to the Committee, the right hon. Member for Birmingham, Hodge Hill tabled a number of amendments—171 to 175 and 177 to 178—that were not selected because they were tabled only yesterday. We need to have several days’ notice before selection can be considered. Had they been tabled earlier, we could have debated and voted on those amendments now. I have given the right hon. Gentleman leeway to widen his arguments about schedule 1, and it is up to him whether he wishes to table those amendments on Report. He is perfectly in order to do so. The debate today is on schedule 1, and the points that the right hon. Gentleman has made in relation to potential amendments are a heads-up for the future or for the Minister to respond to at this point. 

Margot James: The right hon. Member for Birmingham, Hodge Hill covered a lot of important ground. He mentioned the digital charter. We are bringing forward the digital charter and we do not intend for it to be set
in stone. We recognise that this is a fast-changing environment and so it is deliberately something that will evolve over time. We both share the concerns that he expressed with regard to fake news and the rights and protections needed for children and young people who, as he says, make up a third of internet users. We will address many of the things he highlighted as part of our internet safety strategy, and I look forward to debating them further with him on Report.

To add to what we have already discussed under schedule 1, article 9 of the GDPR limits the processing of special categories of data. Those special categories are listed in article 9(1) and include personal data revealing racial or ethnic origin, health, political opinions and religious beliefs. Some of the circumstances in which article 9 says that special category data can be processed have direct effect, but others require the UK to make related provision.

Clause 10 introduces schedule 1 to the Bill, which sets out in detail how the Bill intends to use the derogations in article 9 and the derogation in article 10 relating to criminal convictions data to permit particular processing activities. To ensure that the Bill is future-proof, clause 10 includes a delegated power to update schedule 1 using secondary legislation. Many of the conditions substantively replicate existing processing conditions in the 1998 Act and hon. Members may wish to refer to annexe B to the explanatory notes for a more detailed analysis on that point.

**Darren Jones:** I want to make one point about schedule 1. Amendment 9, which was made this morning, allows democratic engagement to be a purpose under article 6(1)(e) of the GDPR—namely, that consent is not required for the processing of data for public interest or the exercising of official authority and the purposes of democratic engagement. I wonder whether the definitions of political parties and politicians under schedule 1 could be used to restrict that amendment, so that organisations other than political parties and politicians are not able to process data in the public interest for democratic engagement without consent. For example, if Leave.EU or Open Britain wanted to process our personal data, they ought to do so with consent, not using the same public interest for democratic engagement purposes as politicians or parties.

**Margot James:** I understand the hon. Gentleman’s concerns. The GDPR requires data controls to have a legal basis laid down in law, which can take the form, for example, of a statutory power or duty, or a common-law power. Any organisation that does not have such legal basis would have to rely on one of the other processing conditions in article 6. With regard to the amendment that was agreed to this morning, we think that further restricting clause 8 might risk excluding bodies with a lawful basis for processing. However, the hon. Gentleman is free to raise the issue again on Report.

**Question put and agreed to.**

**Schedule 1, as amended, accordingly agreed to.**

**Clauses 11 to 13 ordered to stand part of the Bill.**

**Clause 14**

**Automated decision-making authorised by law; safeguards**

**Liam Byrne:** I beg to move amendment 153, in clause 14, page 7, line 30, at end insert—

“(1A) A decision that engages an individual’s rights under the Human Rights Act 1998 does not fall within Article 22(2)(b) of the GDPR (exception from prohibition on taking significant decisions based solely on automated processing for decisions that are authorised by law and subject to safeguards for the data subject’s rights, freedoms and legitimate interests).”

This amendment would clarify that the exemption from prohibition on taking significant decisions based solely on automated processing must apply to purely automated decisions that engage an individual’s human rights.

**The Chair:** With this it will be convenient to discuss the following:

Amendment 130, in clause 14, page 7, line 34, at end insert—

“(2A) A decision that engages an individual’s rights under the Human Rights Act 1998 does not fall within Article 22(2)(b) of the GDPR (exception from prohibition on taking significant decisions based solely on automated processing for decisions that are authorised by law and subject to safeguards for the data subject’s rights, freedoms and legitimate interests).”

This amendment would ensure that where human rights are engaged by automated decisions these are human decisions and provides clarification that purely administrative human approval of an automated decision does make an automated decision a ‘human’ one.

Amendment 133, in clause 50, page 30, line 5, at end insert “, and

(c) it does not engage the rights of the data subject under the Human Rights Act 1998.”

This amendment would ensure that automated decisions should not be authorised by law if they engage an individual’s human rights.

Amendment 135, in clause 96, page 56, line 8, after “law” insert

“unless the decision engages an individual’s rights under the Human Rights Act 1998”.

**Liam Byrne:** The amendments touch on what I am afraid will become an increasing part of our lives in the years to come: the questions of what decisions can be taken by algorithms; where such decisions are taken, what rights we have to some kind of safeguards, such as a good old-fashioned human being looking over the decision that is taken and the outcomes that arise; and whether we are content to acquiesce in the rule of the robots.

In a number of areas of our lives—particularly our economic and social lives—such algorithms will become more and more important. Algorithms are already used to screen job applications, for example, and to create shortlists of candidates for interview. Insurance companies use them to adjudicate what premiums someone should enjoy, or whether they should be offered insurance at all. The challenge of algorithms was put best by my hon. Friend the Member for Cambridge on Second Reading: the great risk of such developments is that old injustice is hard-coded into new injustice.

That is particularly troubling when we think about the provisions and exemptions the Government have brought forward that allow the automatic processing of data in public services. Many public servants around the world are beginning to look at predictive public services and how algorithms can scan great swathes of, for example, health data and crime data, and make decisions about where police should attend, who should or should not get bail, who should be added to police
as many of us know from our own casework, is a nice
taking. It is okay to use algorithms to inform decisions
but we want fetters around the business of decision
the Government to process data in an automatic way,
W e want to lea ve unfettered the rights of businesses and
is automated, but not for decision taking to be automated.
the possibilities of automatic decision taking. It is fine
an algorithm, all sorts of problems will arise. W e think
police can stop people, search people and put through
the police are authorised to do so much by la w . The
safeguard, particularly when it comes to policing, because
in future by stopping the ability of algorithms to take
stopped the potential for that snowballing of problems
algorithm is wrong.” W e think it would be better if we
been really fouled up . I'm sorry , but either the data that
or indeed with the public agency to say, “Look, this has
2.45 pm
The great risk with automatic processing of data and
the use of algorithms, whether in the public or private
sector, where there is an ex post facto right of review, is
that our surgeries end up as the final court of appeal. It
will then fall to us to intervene either with the company
or indeed with the public agency to say, “Look, this has
been really fouled up. I'm sorry , but either the data that
went into the algorithm is wrong, or the conduct of the
algorithm is wrong.” We think it would be better if we
stopped the potential for that snowballing of problems
in future by stopping the ability of algorithms to take
decisions where human rights are engaged.

The Minister may say that there are lots of nice
safeguards in the Bill, such as that it is permitted only
where it is authorised by law. Frankly, that is a hopeless
safeguard, particularly when it comes to policing, because
the police are authorised to do so much by law. The
police can stop people, search people and put through
procedures that would deny people bail. The police can
add people to databases. If those decisions are taken by
an algorithm, all sorts of problems will arise. We think
that there should be much stronger safeguards.

Through the amendments, basically we want to try to
separate the business of automatic data processing from
the possibilities of automatic decision taking. It is fine
for data to be processed using algorithms in a way that
is automated, but not for decision taking to be automated.
We want to leave unfettered the rights of businesses and
the Government to process data in an automatic way,
but we want fetters around the business of decision
taking. It is okay to use algorithms to inform decisions
but not to take decisions. The idea of a post hoc review,
as many of us know from our own casework, is a nice
idea that is not a reality open to many citizens in this
country. There is no substitute for preventing a decision
being wrong in the first place.

This debate will grow over the years to come. We
hope that the Government can take the opportunity
now to incorporate some fairly common-sense safeguards
into the Bill, because none of us on this Committee
wants old injustices to be hard-coded into new injustices.
That is the risk that the Bill is running.

Brendan O'Hara (Argyll and Bute) (SNP): I will
speak to amendments 130, 133 and 135, which appear
in my name and that of my hon. Friend the Member for
Cumbernauld, Kilsyth and Kirkintilloch East. Our
amendments seek to provide protection for individuals
who are subject to purely automated decision making,
specifically where we believe that it could have an adverse
impact on their fundamental rights. The amendments
would require that where human rights are or possibly
could be impacted by automated decisions, ultimately
there are always human decision makers. The amendments
would instil that vital protection of human rights with
regard to the general processing of personal data.

The amendments seek to clarify the meaning of a
decision that is based solely on automated processing,
which is a decision that lacks meaningful human input.
That reflects the intent of the GDPR, and provides
clarification that purely administrative human approval
of an automated decision does not make that decision a
human one. It is simply not enough for human beings to
process the information in a purely administrative fashion,
but to have absolutely no oversight or accountability for
the decision that they process. We strongly believe that
automated decision making without human intervention
should be subject to strict limitations to ensure fairness,
transparency and accountability, and to safeguard against
discrimination. As it stands, there are insufficient safeguards
in the Bill.

As the right hon. Member for Birmingham, Hodge
Hill said, we are not talking about every automated
decision. We are not talking about a tech company or
an online retailer that suggests alternatives that someone
may like based on the last book they bought or the last
song they downloaded. It is about decisions that can be
made without human oversight that will or may well
have long-term, serious consequences on an individual’s
health, financial status, employment or legal status. All
too often, I fear that automated decisions involve an
opaque, unaccountable process that uses algorithms that
are neither as benign nor as objective as we had
hoped they would be, or indeed, as we thought they
were when we first encountered them.

We are particularly concerned about elements of the
Bill that allow law enforcement agencies to make purely
automated decisions. That is fraught with danger and at
odds with the Data Protection Act 1998, as well as article
22 of the GDPR, which states:

“The data subject shall have the right not to be subject to a
decision based solely on automated processing”.

Although there are provisions in the GDPR for EU
member states to opt out of that, the opt-out does not apply
if the data subject’s rights, freedoms or legitimate
interests are undermined.

I urge the Government to look again at the parts of
the Bill about automated decision making, to ensure
that when it is carried out, a human being will have to
decide whether it is reasonable and appropriate to continue
on that course. That human intervention will provide
transparency and capability, and it will ensure that the state does not infringe on an individual’s freedoms—those fundamental rights of liberty and privacy—which are often subjective. Because they are subjective, they are beyond the scope of an algorithm.

There are serious human rights, accountability and transparency issues around fully automated decision making as the Bill stands. Amendment 130 says that any human involvement has to be “meaningful”. We define meaningful human oversight as being significant, of consequence and purposeful. As I have said, that is far beyond the scope of an algorithm. If an individual’s rights are to be scrutinised and possibly fundamentally affected, it is an issue of basic fairness that the decision is made, or at least overseen, by a sentient being. I hope the Government accept the amendments in the faith in which they were tabled.

Margot James: The amendments relate to automated decision making under the GDPR and the Bill. It is a broad category, which includes everything from trivial things such as music playlists, as mentioned by the hon. Member for Argyll and Bute, and quotes for home insurance, to the potentially more serious issues outlined by the right hon. Member for Birmingham, Hodge Hill of recruitment, healthcare and policing cases where existing prejudices could be reinforced. We are establishing a centre, the office for artificial intelligence and data ethics, and are mindful of these important issues. We certainly do not dismiss them whatsoever.

Article 22 of the GDPR provides a right not to be subject to a decision based solely on automatic processing of data that results in legal or similarly significant effects on the data subject. As is set out in article 22(2)(b), that right does not apply if the decision is authorised by law, so long as the data subject’s rights, freedoms and legitimate interests are safeguarded.

The right hon. Member for Birmingham, Hodge Hill, mentioned those safeguards, but I attribute far greater meaning to them than he implied in his speech. The safeguards embed transparency, accountability and a right to request that the decision be retracted, and for the data subject to be notified should a decision be made solely through artificial intelligence.

Liam Byrne: The Minister must realise that she is risking an explosion in the number of decisions that have to be taken to Government agencies or private sector companies for review. The justice system is already under tremendous pressure. The tribunal system is already at breaking point. The idea that we overload it is pretty optimistic. On facial recognition at public events, for example, it would be possible under the provisions that she is proposing for the police to use facial recognition technology automatically to process those decisions and, through a computer, to have spot interventions ordered to police on the ground. The only way to stop that would be to have an ex post facto review, but that would be an enormous task.

Margot James: The right hon. Gentleman should be aware that just because something is possible, it does not mean that it is automatically translated into use. His example of facial recognition and what the police could do with that technology would be subject to controls within the police and to scrutiny from outside.

Louise Haigh: The case that my right hon. Friend raises is certainly not hypothetical. The Metropolitan police have been trialling facial recognition scanning at the Notting Hill carnival for the last three years with apparently no legal base and very little oversight. We will move on to those issues in the Bill. That is exactly why the amendments are crucial in holding law enforcement agencies to account.

Margot James: As the hon. Lady says, the police are trialling those things. I rest my case—they have not put them into widespread practice as yet.

Returning to the GDPR, we have translated the GDPR protections into law through the Bill. As I said, the data subject has the right to request that the decision be retracted with the involvement of a sentient individual. That will dovetail with other requirements. By contrast, the amendments are designed to prevent any automated decision-making from being undertaken under article 22(2)(b) if it engages the rights of the data subject under the Human Rights Act 1998.

Liam Byrne: Will the Minister explain to the Committee how a decision to stop and search based on an automated decision can be retracted? Once the person has been stopped and searched, how can that activity be undone?

Margot James: I am not going to get into too much detail. The hon. Member for Sheffield, Heeley mentioned an area and I said that it was just a trial. She said that facial recognition was being piloted. I do not dispute that certain things cannot be undone. Similar amendments were tabled in the other place. As my noble Friend Lord Ashton said there, they would have meant that practically all automated decisions under the relevant sections were prohibited, since it would be possible to argue that any decision based on automatic decision making at the very least engaged the data subject’s right to have their private life respected under article 8 of the European convention on human rights, even if it was entirely lawful under the Act.

3 pm

Amendment 130 also seeks to clarify what is meant by a decision “based solely on automated processing” to ensure that human intervention must be meaningful. We consider the amendment unnecessary, as the phrase, especially when read with recital 71 of the GDPR, already provides for this. As my noble Friend Lord Ashton stated in the other place, “merely human presence or incidental human involvement is not sufficient”—[Official Report, House of Lords, 13 December 2017; Vol. 787, c. 1581.]

Margot James: To change the basis of a decision. I am very happy to put that on the record once more. However, even if it were not the case, we could not go around altering definitions under the GDPR; it is not in our gift to do so.

Liam Byrne: I fear that the Minister is taking some pretty serious gambles on the application of this technology in the future. We think it is the business of this place to ensure that our citizens have strong safeguards, so we will put the amendment to a vote.
The Committee divided: Ayes 9, Noes 10.

Division No. 3]

AYES
Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren
McDonald, Stuart C.

Murray, Ian
O'Hara, Brendan
Snell, Gareth
Zeichner, Daniel

NOES
Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

Jack, Mr Alister
James, Margot
Lopez, Julia
Warman, Matt
Wood, Mike

Question accordingly negatived.

The Chair: Does the hon. Member for Argyll and Bute wish to press amendment 130 to a Division?

Brendan O’Hara: I would like to press the amendment to a vote, or should I do that on Report?

The Chair: The hon. Gentleman can press the amendment to a vote now. If it is carried, it will be part of the Bill. If it is defeated, it will not be, and it may then be moved on Report, subject to the Speaker’s discretion. If the hon. Gentleman does not press the amendment now, it may be that there is more of a likelihood of its being picked on Report, but that is a matter for the Speaker.

Brendan O’Hara: In that case, I will not press the amendment now.

Margot James: I beg to move Government amendment 10, in clause 14, page 8, line 4, leave out “21 days” and insert “1 month”.

Clause 14(4)(b) provides that where a controller notifies a data subject under ‘Clause 14(4)(a) that the controller has taken a “qualifying significant decision” in relation to the data subject based solely on automated processing, the data subject has 21 days to request the controller to reconsider or take a new decision not based solely on automated processing. This amendment extends that period to one month.

The Chair: With this it will be convenient to discuss Government amendments 11, 12, 23, 24, 27, 28, 41 and 42.

Margot James: Amendments 10, 11 and 12 relate to clause 14, which requires a data controller to notify a data subject of a decision based solely on automatic processing as soon as is reasonably practicable. The data subject may then request that the controller reconsider such a decision and take a new decision not based solely on automated processing.

The purpose of the amendments is to bring clause 14 into alignment with the directly applicable time limits in article 12 of the GDPR, thereby ensuring that both data subjects and data controllers have easily understandable rights and obligations. Those include giving the data subject longer to request that a decision be reconsidered, requiring that the controller action the request without undue delay and permitting an extension of up to two months where necessary.

Furthermore, to ensure that there is consistency across the different regimes in the Bill—not just between the Bill and the GDPR—amendments 23, 24, 41 and 42 extend the time limit provisions for making and responding to requests in the other regimes in the Bill. That is for the simple reason that it would not be right to have a data protection framework that applies one set of time limits to one request and a different set of time limits to another.

In a similar vein, amendments 27 and 28 amend part 3 of the Bill, concerning law enforcement processing, to ensure that controllers can charge for manifestly unfounded or excessive requests for retaking a decision, as is permitted under article 12 of the law enforcement directive. To prevent abuse, amendment 28 provides that it is for the controller to be able to show that the request was manifestly unfounded or excessive.

Liam Byrne: It would be useful if the Minister could say a little more about the safeguards around the controllers charging reasonable fees for dealing with requests.

It is quite easy to envisage situations where algorithms take decisions. We have some ex post facto review; a citizen seeks to overturn the decision; the citizen thinks they are acting reasonably but the commercial interest of the company that has taken and automated the decision means that it wants to create disincentives for that rigmarole to unfold. That creates the risk of unequal access to justice in these decisions.

If the Minister is not prepared to countenance the sensible safeguards that we have proposed, she must say how she will guard against another threat to access to justice.

Margot James: The right hon. Gentleman asks a reasonable question. I did not mention that data subjects have the right of complaint to the Information Commissioner if the provisions are being abused. I also did not mention another important safeguard, which is that it is for the data controller to show that the request is manifestly unfounded or excessive. So the burden of proof is on the data controller and the data subject has the right of involving the Information Commissioner, if he or she contests the judgment taken in this context, concerning unfounded or excessive requests in the opinion of the data controller. I hope that satisfies the right hon. Gentleman.

Amendment 10 agreed to.

Amendments made: 11, in clause 14, page 8, leave out line 10 and insert “within the period described in Article 12(3) of the GDPR—”.

This amendment removes provision from Clause 14(5) dealing with the time by which a controller has to respond to a data subject’s request under Clause 14(4)(b) and replaces it with a requirement for the controller to respond within the time periods set out in Article 12(3) of the GDPR, which is directly applicable.

Amendment 12, in clause 14, page 8, line 16, at end insert—

(5A) In connection with this section, a controller has the powers and obligations under Article 12 of the GDPR (transparency, procedure for extending time for acting on request, fees, manifestly unfounded or excessive requests etc) that apply in connection with Article 22 of the GDPR.” —[Margot James.]
This amendment inserts a signpost to Article 12 of the GDPR which is directly applicable and which confers powers and places obligations on controllers to whom Clause 14 applies.

Clause 14, as amended, ordered to stand part of the Bill.

Clause 15
Exemptions etc.

Margot James: I beg to move amendment 13, in clause 15, page 8, line 31, after “21” insert “and 34”
This amendment is consequential on Amendment 94.

The Chair: With this it will be convenient to discuss Government amendments 14, 93 to 106, 109, 110 and 112.

Margot James: Schedule 2 allows for particular rights or obligations contained in the GDPR to be disappplied in particular circumstances, where giving effect to that right or obligation would lead to a perverse outcome. To do that, it makes use of a number of derogations in the GDPR, including articles 6(3) and 23(1).

Amendments 93, 95 and 109 permit article 19 of the GDPR to be disappplied for the purposes in parts 1, 2 and 5 of schedule 2.

When a data controller corrects or deletes personal data following a request from a data subject, article 19 of the GDPR requires them to inform all persons to whom the personal data has been disclosed. Additionally, if requested, the data controller must inform the data subject about those persons to whom the data has been disclosed. Following the introduction of the Bill, we have had further representations from a range of stakeholders, including the banking industry, regulators and the media sector, about the problems that article 19 might create in very particular circumstances.

The amendments will ensure that, for example, where a bank may have shared personal data about one of its customers with the National Crime Agency because of a suspected fraud, it will not have to tell the data subject about that disclosure when the customer changes their address with the bank. That will ensure that the data subject is not tipped off about the suspected fraud investigation.

Several amendments in the group are designed to ensure that a valuable provision of the GDPR—article 34—does not have unintended consequences for controllers who do the right thing by seeking to prevent or detect crime, assist with the assessment or collection of tax or uncover abuses in our society. Article 34 requires data controllers to inform a data subject if there has been a data breach that is likely to result in a high risk to the rights and freedoms of an individual. In normal operation, this is an important article, which we hope will prompt a step change in the way organisations think about cyber-security.

However, article 23(1) enables member states to create laws to restrict the scope of the obligations and rights for which article 34 provides in the minority of cases where it conflicts with other important objectives of general public interest. The amendments seek to do that in the Bill. Amendment 94 responds to the concerns of the finance sector that compliance with article 34 may result in persons under investigation for financial crime being tipped off. Amendment 110 serves a similar purpose for media organisations.

Article 85(2) creates scope for member states to provide exemptions from chapter 4 of the GDPR, which includes article 34, if they are necessary to reconcile the right to the protection of personal data with the freedom of expression. The amendment intends to ensure that processing data for a special purpose that is in the public interest is not prejudiced—for example, by a controller having to notify the data subject of a breach in relation to pre-publication undercover footage. Importantly, data controllers will still be required, for the first time, to report a breach to the Information Commissioner under article 33 of the GDPR. That will ensure that she is well placed to take all the necessary steps to ensure data subjects’ rights are respected, including by monitoring compliance with these new exemptions.

On the more general question of who can make use of the exemptions in schedule 2 and when, amendment 96 broadens the exemption in paragraph 7 of the schedule, which relates to the protection of members of the public. As drafted, the exemption applies to personal data processed for the purposes of discharging a function that is designed to protect members of the public against dishonesty, malpractice or incompetence by persons who carry out activities that bring them into contact with members of the public. We have identified an issue with that wording: a number of public office holders, including police staff, do not carry out activities that necessarily bring them into contact with members of the public. Amendment 96 broadens the scope of the exemption to include processing in relation to individuals who work for those organisations in a behind-the-scenes capacity.

We have also had representations from several regulators on the need to make additional provisions to protect the integrity of their activities. Amendment 97 provides the UK’s Comptroller and Auditor General, and their counterpart in each of the devolved Administrations, with an exemption from certain GDPR provisions where these are likely to prejudice their statutory functions. That will prevent certain individuals who suspect they may be under scrutiny from trying to use their rights under the GDPR, such as article 15 (confirmation of processing) as a way of confirming that their data is being processed, or from using article 17 (right to erasure) and article 18 (restriction of processing) to undermine the effectiveness of an audit.

3.15 pm

Likewise, amendment 98 provides an exemption for the Bank of England from the list of GDPR provisions, where these may inhibit its ability to exercise its functions. This amendment ensures the Bank of England can continue its work as a monetary authority without undue restriction from the GDPR. Amendments 99 and 100 are technical changes, which clarify that the table in paragraph 9 of schedule 2 refers to persons rather than bodies, to reflect the legal characteristics of the listed regulators. Amendment 101 adds section 244 of the Investigatory Powers Act 2016 to the list of legislation that confers processing functions on the Information Commissioner. Section 244 requires the commissioner to audit compliance, with certain obligations imposed by part 4 of the Investigatory Powers Act. This amendment would therefore exempt the commissioner from certain provisions of the GDPR in respect of those oversight functions. Hon. Members will agree that the commissioner’s powers of oversight are vital to
her being an effective regulator. This amendment will allow her to use her investigatory powers in an unrestricted manner, to ensure compliance with the rules around the retention of data.

Amendment 102 provides an exemption for the Scottish Information Commissioner. A similar provision already exists for the UK Information Commissioner. This was included to address the risk to the UK commissioner’s functions under the various access to information regimes, which could be prejudiced in some circumstances if she were to comply with a full range of the data subject’s rights. The Scottish commissioner has confirmed that the same rights exist when carrying out his functions under equivalent Scottish legislation. We have therefore drafted this amendment to provide the Scottish Information Commissioner with an equivalent exemption to that of the UK Information Commissioner in relation to these functions.

Amendment 104 creates protection for the Financial Conduct Authority and the Prudential Regulation Authority. Clearly such protection is necessary for the integrity of our financial services’ regulatory landscape. Amendment 105 extends the exemptions in schedule 2 to the Charity Commission’s functions under the Charities Act 1992, the Charities Act 2006 and the Charities Act 2011. Again, these exemptions apply only where a right or obligation would be likely to prejudice the ability to discharge a function conferred on them by statute. Amendments 106 and 112 relate to schedule 3, which provides for restrictions from certain GDPR provisions where this is necessary for health, education and social work purposes.

Paragraph 16 provides an exemption from certain GDPR provisions in relation to educational records in Northern Ireland. It currently applies only to information processed by or on behalf of the board of governors or a teacher at a grant-aided school. This amendment extends the exemption so that it includes records of information processed by or on behalf of grant-aided and independent school regardless of their governance arrangements.

Amendment 13 agreed to.

Amendment made: 14, in clause 15, page 8, line 34, after “21” insert “and 34”. — (Margot James.)

This amendment is consequential on an amendment made in the Lords which added Article 34 of the GDPR (communication of personal data breach to the data subject) to the list of GDPR provisions that are disapplied by paragraph 11 of Schedule 2 to the Bill.

Clause 15, as amended, ordered to stand part of the Bill.

Schedule 2

EXEMPTIONS ETC FROM THE GDPR

Amendments made: 93, in schedule 2, page 135, line 7, at end insert—

( ) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing); This amendment adds Article 19 of the GDPR (notification obligation regarding rectification or erasure of personal data or restriction of processing) to the list of GDPR provisions that are disapplied by provisions in Part 1 of Schedule 2 to the Bill.

Amendment 94, in schedule 2, page 135, line 19, after “provisions” insert—

“and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject)” —(Margot James.)
underfunded by the Treasury. They have been underfunded by the Treasury under this Government and, in my view, we did not get enough out of the Treasury in my day.

However, they are human and make mistakes. That is why we have such a complicated immigration tribunal system, where people can take their complaints to a first tier tribunal but very often need to seek a judicial review down the line. The challenge is that, if the Home Office wants to create a process and an administration for making the right decision, which can be defended in a tribunal and in a judicial review case, that process must be robust. When we streamlined the immigration tribunal system, we realised that we had to change, improve and strengthen the way that we took decisions in the Home Office because too many were made in a way that was not JR-proof. We were losing JR s and therefore denying justice to those who brought a legitimate claim against the Crown.

There were occasions when I lost cases because of information that was disclosed to the applicant through a subject access review. SARs are one of the most powerful instruments by which anybody in this country, whether a citizen or someone applying to become a citizen, or applying for a legal right to remain, can acquire information that is crucial to the delivery of justice. Many of us are incredibly sympathetic to the job that the Home Office does. Many of us will want a tougher regime in policing immigration, in particular illegal immigration, but I suspect every member of the Committee is also interested in the good conduct of justice and administrative justice. As someone who served in the Home Office for two years, I had to take some very difficult decisions, including to release subject access request information that I absolutely did not want to go into the public domain. Sometimes it was right to release that information because it helped ensure that justice was done in the courts of this land.

The Minister has some very strong safeguards in the Bill. There are strong safeguards that create exemptions for her where the interest is in crime prevention, such as, for example, illegal immigration. However, the power that the provision seeks, at which we take aim in our amendments, is a step too far and risks the most terrible injustices. It risks the courts being fouled up and our being challenged in all sorts of places, including the European Court of Human Rights in the years to come. It is an unwise provision. If I were a Home Office official, I would have tried it on—I would have tried to get it through my Minister and through the Houses of Parliament, but it is unwise and a step too far. I hope the Minister will accept the amendment and delete the provisions.

Brendan O’Hara: I will speak in favour of amendment 156. On Second Reading, I said that I would raise this matter again in Committee and I make no apologies for doing so. We regard this new exemption as extremely concerning. It permits the Government to collect and hold data for the purposes of what they describe as “effective immigration.”

It also concerns me that nowhere in the Bill does there seem to be a legal definition of effective immigration control. I am worried that “effective immigration control” is highly subjective and highly politicised. It exposes individuals, weakens their rights and makes them vulnerable to whatever change in the political tide happens to come along next. This broad-ranging exemption is fundamentally unfair. It is open to abuse and runs contrary to safeguarding basic human rights. I believe that the UK’s proposed immigration exemption goes much further than the scope of restrictions afforded to member states under GDPR, with all the consequences of that, which we discussed in such great detail this morning around adequacy decisions.

3.30 pm

The exemption would introduce a new and unprecedented removal of an individual’s data protection rights and it is as unnecessary as it is disproportionate. Under this exemption, the Government will remove any obligation they have under data protection to inform an individual that their data has been transferred to the Home Office for immigration control purposes. That individual would not know if their data was being held or whether they were under investigation. That individual would have no right to know what data was being held by the Home Office or why. They would have no way of checking the accuracy of the information being held and therefore no way of correcting any mistakes in the information, which could then be used by the Home Office to decide whether they could live in this country or not.

Ian Murray (Edinburgh South) (Lab): The hon. Gentleman makes a powerful case against this particular exemption. He will know as well as me as a constituency Member of Parliament that one of the first things checked when someone comes to seek our advice is whether the Home Office has the correct information on an individual. Nine times out of 10, because of sheer workload, the Home Office just has it wrong. Then the visas and so on can be processed. Am I right in saying that, under this exemption, we would be unable to do that?

Brendan O’Hara: The hon. Gentleman is absolutely correct; I was just getting on to the point about the information held by the Home Office. It cannot be checked and if it is wrong at source, it is wrong at the end of the process. As far as I can see, there are no safeguards against that. He is absolutely correct that one early error in data collection and processing becomes an irrefutable and indisputable fact by the time it reaches the Home Office. The Home Office could then base its case against an individual on that wrong information.

The hon. Gentleman is right—as constituency MPs, there is not one of us, I am sure, who is not painfully aware of wrong information being held not just by the Home Office, but by a whole range of Departments. That makes the exemption fundamentally unfair. This is an issue of basic fairness and there is little wonder it has been so loudly and roundly condemned by civil liberties groups and many in the legal profession. If we go ahead with the schedule as it stands, it fundamentally changes how we can operate and how we can help people who require our assistance.

At the moment, we have subject access requests. As matters stand, the Home Office and the subject or their legal representative have a right to access the same information, on which legal claims and challenges are based. Surely, if both sides do not have access to the same information, the fairness of any legal proceedings is inevitably compromised. Subject access requests are
often the only route through which a legal professional can make representations on very complicated issues on behalf of their client. Indeed, for clients who have been victims of domestic abuse and are fleeing an abusive partner, sometimes a subject access request is all that stands between them and a successful application to remain. This exemption will reduce legal representatives’ ability to best represent their clients and it removes a fundamental tool for holding the Home Office to account when it either gets things wrong or chooses to ignore or misrepresent the facts. The exemption is fundamentally unfair and as unnecessary as it is disproportionate. I urge the Government to reconsider.

Darren Jones: I support the amendment tabled by my right hon. and hon. Friends, because there are some harsh realities about this exemption for effective immigration control, including the harsh reality that such an exemption right does not exist under the GDPR. Indeed, it is a new exemption compared with the law that exists today under the Data Protection Act 1998.

This broad, undefined exemption really must be restricted. I declare an interest. My wife is Australian and is here on a spousal visa. I therefore assume that, as a British citizen, I too could be subject to my rights being exempted for the effective control of immigration in order to understand what my wife is up to. I should declare for the record that her staying here in the UK is perfectly legitimate. This is a wide-ranging exemption that could apply to EU citizens, non-EU citizens and, as I say, British citizens who are connected with those who are subject to immigration controls.

This is not just an issue for the Home Office; there is data across various Departments that could be of use to the Home Office for the effective control of immigration. Indeed, we have been waiting for quite some time for the Government to publish the biometric strategy, setting out how they intend to use lots of biometric data across Government Departments. We have been waiting for a couple of years to see how the Government intend to do that.

My understanding is that if all the photographs held on our passports and driving licences were collated, in essence the Government would have the power to have a virtual ID card for the bulk of the adult population in this country. How on earth would that information be used for the effective control of immigration, which would potentially be applied to so many people here in the UK?

This exemption creates a derogation for many rights: the right to information, the right to access, the right to explanation, the right to erasure, the right to restriction of processing, the right to data portability, the right to object, and all the principles set out in article 5 of the GDPR. This is an enormous derogation from rights that our colleagues in Europe think are important. Again, this relates to the risk of failing to seek adequacy in our negotiations with the EU.

I seek not only to support the amendment but to ask the Minister to clarify something. If the Government do not support the amendment, how does the exemption fit within the language of article 23 of the GDPR, which states that it can only exist—

“when such a restriction respects the essence of the fundamental rights”—

which we have already noticed today are being repealed by this Government—

“and freedoms and is a necessary and proportionate measure in a democratic society”? My assertion is that this exemption goes too far and, therefore, that the amendment tabled by my right hon. and hon. Friends is perfectly sensible. I look forward to it receiving Government support.

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): We have already heard three very good speeches in support of the amendment. I will not take too long to support pretty much everything that has been said so far. As a former troublesome immigration lawyer from back in the day—in fact, when the right hon. Member for Birmingham, Hodge Hill was busy making his reforms in the Department—I do not think that I could have lived it down if I had not said a few words in support of the amendment.

We must remember that the context of all this is that we have a Department—the Home Office—where, as the most recent statistics show, half of all immigration decisions that are challenged in a tribunal are overturned, which is a record high. The Home Affairs Committee has recently expressed grave concerns about the poor quality of decision making in far too many areas and the functioning of a hostile environment, for example in the area of bank checks, where there is something like a 10% error rate. We also live in a world where the creeping reach of the Home Office’s information tentacles is almost being seen to put off migrants from accessing necessary public services such as health, creating a public health danger.

To provide a massive and almost unlimited exemption from many of the key protections, as has been described, is not only unjustified but counterproductive, because rather than fixing the fundamental problems with Home Office decision making, it will make them worse by hiding them from view and from scrutiny. The Home Office, not for the first time, is being pretty greedy with the powers that it seeks, because even if we take out the exemption, as this amendment proposes, the Home Office will still have plenty of scope—perhaps too much scope—to do what it wants to do. Recent immigration Acts have created myriad criminal offences in the sphere of immigration law, so the Home Office can already rely on other exemptions within the Bill where necessary. What is absolutely lacking is any explanation of why the exemption is needed. Will the Minister explain what it is about current data protection laws that has unacceptably hindered Home Office operations? I have seen no evidence of that at all.

Another concern is that it is not just the Home Office that will benefit from this exemption but other organisations that are involved in immigration control, such as G4S in its operation of detention centres. There is no justification for that, but there are serious risks, harms and injustices that might be created by the proposed exemption.

As we have heard, subject access requests are regularly a crucial part of representing a migrant caught up in the immigration system. They can be used to establish statuses that have not been communicated or have been lost. They can be used to establish other crucial facts that have not been known to that individual or their representatives. They can, of course, be absolutely crucial in establishing that the Home Office has made errors, as all too many hon. Members will have experienced.
Members of the Committee have been provided with a host of examples by the Law Society, the Bar Council, the Immigration Law Practitioners’ Association and others. Those are real-life examples occurring day in, day out. Quite simply, the failure to allow those individuals access to data protection rights is not only a denial of those rights but a denial of access to justice altogether. This part of the Bill desperately needs reconsideration by the Government.

Victoria Atkins: I feel I should defend all the hardworking people both in the Home Office and Border Force who do their best to do their jobs, day in, day out, to ensure that we have an effective, fair and proportionate immigration system. They have come under a bit of an attack in this debate.

Ian Murray: I do not think anybody on the Committee would disagree with the statement that the staff work incredibly hard. Would it not be a show of solidarity with those staff to give them the resources they require to do the job properly?

Victoria Atkins: The hon. Gentleman is starting the debate in very sparky form.

Ian Murray: You started it.

Victoria Atkins: I didn’t start it. The point is that, when people talk obliquely about the Home Office, it is people working in the Home Office who have to make these decisions day in, day out and who have to apply the law and do their best. I think we need to bear that in mind when we are talking about the Home Office system and how bad it is.

The provision relating to data processing for the purposes of immigration control in paragraph 4 of schedule 2 has been the subject of much debate. I would like to address some of the misunderstandings that have clearly arisen during the course of the Bill around both the purpose and scope of the provision. I hope I can persuade the Committee that this is a necessary and proportionate measure to protect the integrity of our immigration system.

Mr Alister Jack (Dumfries and Galloway) (Con): Opposition Members have expressed concern, which I would like to emphasise, that this exemption is too wide. Can the Minister provide an assurance that that is not the case?

Victoria Atkins: Very much so. I will take it slowly because it is complicated and I want to ensure that the points raised today have been addressed. First, I was asked who decides the definition of effective immigration control in the schedule. That is an established term of art. It is used, for example, in the Immigration Act 2014. The Freedom of Information Act 2000 uses a similar term, namely “the operation of the immigration controls”.

In the context of the schedule, we have adopted a wraparound term such as that, rather than set out a detailed list of specific immigration-related functions to which the exemption might be applied. Given the undoubted complexity of immigration legislation, there is a danger that any such list would be incomplete and would need to be regularly reviewed and updated. The term is either the precise term or similar to those already in law, such as in the Freedom of Information Act, which has been law for 18 years.

The hon. Member for Argyll and Bute seems concerned that once the Home Office system has accessed some of this information, it is lost forever and will not be revealed to the person whom it concerns. I will give case examples later, but I reassure him that the way in which we describe this exemption in the Home Office is that it is a pause on two of the data protection principles. Once the pause is lifted, because the end has been achieved—the person has been found or whatever—all those rights kick back in again, and they are able to make requests for the information that the hon. Gentleman set out. We see it as a pause, not as a long-standing and permanent exemption. It is just for the precise circumstances of enabling the immigration system and its protections.

3.45 pm

Liam Byrne: The Under-Secretary of State will know better than anybody that there are very tight time limits over the windows within which people can ask for entry clearance officer reviews or reconsideration, either by an immigration official or, in extremis, by the Minister. How long will the pause last, and can she guarantee the Committee today that the pause will never jeopardise the kick-in of time limits on an appeal or a reconsideration decision?

Victoria Atkins: The reason for the pause is—I will give case studies of this—to enable the immigration system to operate. If someone has gone missing, requests for data will be required to find that person. Once that person is found, and there is no longer a need to apply the exemption, it will be lifted.

Liam Byrne: That is not an answer to my question. I am asking for a guarantee to the Committee this afternoon that the pause will never jeopardise somebody’s ability to submit a valid request for a reconsideration or an appeal with the information that they need within the time windows set out by Home Office regulations—yes or no.

Victoria Atkins: I am asked whether this will have an impact on someone’s application, either at appeal or reconsideration. Of course, information is obtained so that a person can be brought in. As I say, I will make it clear with case studies, so perhaps I can answer the right hon. Gentleman in more detail when I give such an example, but the purpose of this is generally to find a person. When the need, as set out under the exemption, no longer exists, the rights kick back in again. This relates only to the first two data protection principles under the GDPR. Again, I will go into more detail in a moment, but this is not the permanent exemption from rights as perhaps has been feared by some; it is simply to enable the process to work. Once a person has been brought into the immigration system, all the protections of the immigration system remain.

Stuart C. McDonald: The circumstances that the Minister describes for using the exemption are much narrower than the way the exemption is actually drawn. It seems to me that if that is the only way in which the Home Office wants to use the exemption, it could frame it in a much narrower way and possibly gain cross-party support.
Victoria Atkins: I will move on to the case studies in a moment, as I have given way several times. First, I will lay out the titles, then I will come on to article 23. Again, our analysis is that the provision fits within one of the exemptions in article 23. That is precisely the reason that we have drawn it in this way.

We very much welcome the enhanced rights and protections for data subjects afforded by the GDPR. The authors of the GDPR accepted that at times those rights need to be qualified in the public interest, whether to protect national security, the prevention and detection of crime, the economic interests of the country, or, in this case, the maintenance of an effective system of immigration control. Accordingly, a number of articles of the GDPR make express provision for such exemptions, including article 23(1)(e), which enables restrictions to be placed on certain rights of data subjects. Given the extension of data subjects’ rights under the GDPR, it is necessary to include in the Bill an explicit targeted but proportionate exemption in the immigration context.

The exemption would apply to the processing of personal data by the Home Office for the purposes of “the maintenance of effective immigration control, or...the investigation or detection of activities that would undermine the maintenance of effective immigration control”. It would also apply to other public authorities required or authorised to share information with the Department for either of those specific purposes.

Let me be clear on what paragraph 4 of schedule 2 does not do. It categorically does not set aside the whole of the GDPR for all processing of personal data for all immigration purposes. It makes it clear that the exemption applies only to certain GDPR articles. The articles that the exemption applies to are set out in paragraph 4(2) of schedule 2. They relate to various rights of data subjects provided for in chapter 3 of the GDPR, such as the right to request access in article 15; the right to object in article 21(1); the principle of lawful, fair and transparent processing in article 5; the principle of purpose limitation in article 5(1)(b); and the data protection principles in article 5 of lawful, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability to the extent that they correspond to the rights above. That is a pretty broad set of rights to be cast out.

Liam Byrne: As I understand it, the derogations that are sought effectively remove the right to information in article 13; the right to information where data is obtained from a third party in article 14; the right of subjects’ access in article 15; the right to erase in article 17; the right to restriction of processing in article 18; the right to object in article 21(1); the principle of lawful, fair and transparent processing in article 5; the principle of purpose limitation in article 5(1)(b); and the data protection principles in article 5 of lawful, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability to the extent that they correspond to the rights above. That is a pretty broad set of rights to be cast out.

Victoria Atkins: Those are not the data protection principles. If one continues to read on to paragraph 4(2)(b) of schedule 2, it sets out the two data protection principles that I have just highlighted. The provisions set out in sub-paragraph (2)(a) relate to the data protection principles of fair and transparent processing and the purpose limitation. As I say, this is not a permanent removal. This is, as we describe it, a pause. There is not a free hand to invoke the permitted exception as a matter of routine.

All of the data protection principles, including those relating to data minimisation, accuracy, storage limitation and integrity and confidentiality, will continue to apply to everyone. So, too, will all the obligations on controllers and processors, all the safeguards around cross-border transfers, and all the oversight and enforcement powers of the Information Commissioner. The latter is particularly relevant here, as it is open to any data subject affected by the provisions in paragraph 4 of schedule 2 to make a complaint to the Information Commissioner that the commissioner is then under a duty to investigate. Again, I hope that that addresses some of the concerns that the hon. Member for Argyll and Bute raised.

Contrary to the impression that has perhaps been given or understood, paragraph 4 does not give the Home Office a free hand to invoke the permitted exceptions as a matter of routine. The Bill is clear that the exceptions may be applied only to the extent that the application of the rights of data subjects, or the two relevant data protection principles, would be likely to prejudice “the maintenance of effective immigration control, or...the investigation or detection of activities that would undermine the maintenance of effective immigration control”. That is an important caveat.

Liam Byrne: The Minister will know that in paragraph 2(1)(a) we already have a set of exemptions that relate to the prevention or detection of a crime, including, presumably, all of the crimes that fall into the bucket of organising or perpetrating illegal immigration. Despite constant pressing during the debate in the other place and here, we have not yet had a clear answer as to why additional powers and exemptions are needed, over and above the powers expressly granted and agreed in paragraph 2(1)(a).

Victoria Atkins: I am grateful to the right hon. Gentleman for raising that issue, because it allows me to get to the nub of how we approach the immigration system. We do not see the immigration system as some form of criminality or as only being open to the principles of criminal law. He will know that we deal with immigration in both the civil law and criminal law contexts. The exemption he has raised in terms of paragraph 2 of the schedule deals with the criminal law context, but we must also address those instances where the matter is perhaps for civil law.

We know that in the vast majority of immigration cases, people are dealt with through immigration tribunals or through civil law. They are not dealt with through criminal law. That is the point; we must please keep open the ability to deal with people through the civil law system, rather than rushing immediately to criminalise them. If, for example, they have overstayed, sometimes it is appropriate for the criminal law to become involved, but a great number of times it is for the civil law to be applied to deal with that person’s case either by way of civil penalty or by finding an arrangement whereby they can be given discretion to leave or the right to remain. We have the exemption in paragraph 4 so that we do not just focus on the criminal aspects that there may be in some immigration cases. We must ensure that we also focus on the much wider and much more widely used civil law context.

It is important to recognise that the exemptions will not and cannot be targeted at whole classes of vulnerable individuals, be they victims of domestic abuse or human
trafficking, undocumented children or asylum seekers. The enhanced data rights afforded by the GDPR will benefit all those who are here lawfully in the United Kingdom, including EU citizens. The relevant rights will be restricted only on a case-by-case basis where there is evidence that the prejudice I have mentioned is likely to occur.

Peter Heaton-Jones (North Devon) (Con): The Minister specifically mentioned EU citizens. There have been concerns that the exemption will impact those EU nationals who are already here and who, as we have already heard, are contributing hugely to the UK. Can she assure us that the exemption is not targeted at them?

Victoria Atkins: Absolutely. The exemption will not be enacted on the basis of nationality. It is enacted on a case-by-case basis to uphold the integrity of the immigration system. There will be no question of EU nationals being in any way targeted by it. Indeed, we know the great effect that EU nationals and other people from other countries have had in this country, and we certainly would not be looking to target them on the basis of nationality.

Darren Jones: Is it not right to say that EU citizens will be part of the immigration system? They will be immigrants with immigration rights as part of the Brexit process. These rules could therefore apply to them, could they not? Secondly—

Victoria Atkins: I will answer the first one—yes. The hon. Gentleman asked whether EU citizens would be targeted. Once we leave the European Union, we will have our own immigration policy. There will clearly be no distinction between EU and non-EU, because everyone will be outside of the UK, if I may put it that way, very inelegantly.

Darren Jones: But they would still be subject to the right to exempt them from their data protection rights. I welcome the Minister’s comments on the time-limited nature of the intention of using the rules, but can she point me to the section of the Bill that defines that time limit, because I am struggling to find it?

Victoria Atkins: If I may, I will come back to that point in a moment. In the case of subject access requests, each request would need to be considered on its own merits. For example, we could not limit the information given to visa applicants on how their personal data would be processed as part of that application. Rather, the restrictions would be applied only where there was a real likelihood of prejudice to immigration controls as a result of disclosing the information concerned.

4 pm

It is equally important to shed light on another concern that has been voiced. Some of the briefing that has been circulated suggests that the Bill creates new information sharing gateways. That is simply not the case. As I have indicated, schedule 2 sets out certain exceptions from GDPR. It does not of itself create new powers to share data between data controllers. However, where personal data is shared between controllers for the limited immigration purposes specified in paragraph 4, it means that the data subject does not need to be notified, if to do so would be prejudicial to the maintenance of effective immigration control.

It may assist the Committee if I explain the kind of information that it may be necessary to withhold from data subjects. The classes of information that the Home Office may wish to withhold include a description of the data held, our data sources, the purposes for which that data is being processed, and the details of the recipients to whom the data has been disclosed. There will be circumstances in which the disclosure to a data subject of such information could afford him or her the opportunity to circumvent our immigration controls. A couple of examples will serve to illustrate where the disclosure of such information may have precisely that adverse effect.

In the case of a suspected overstayer, if we had to disclose, in response to a subject access request, what we are doing to track their whereabouts with a view to effecting administrative removal—that is the difference from the paragraph 2 point that the right hon. Member for Birmingham, Hodge Hill highlighted—evidently, that would tip them off, and thus undermine such enforcement action.

Liam Byrne: If someone has overstayed, they have committed a crime. Therefore, paragraph 2(1)(a) absolutely bites. We are seeking to prevent that crime. Someone who has overstayed their visa has committed a crime. It is kind of as simple as that.

Victoria Atkins: In that scenario, we may well effect their removal administratively. It does not mean that it is going through the criminal courts.

By way of a second example, take a case where the Home Office is considering an application for an extension of leave to remain in the UK. It may be that we have evidence that the applicant has provided false information to support his or her claim. In such cases, we may need to contact third parties to substantiate the veracity of the information provided in support of the application. If we are then obliged to inform the claimant that we are taking such steps, they may abscond and evade detection.

Liam Byrne: If someone has submitted false information in support of an application to the Government, and signed it, as they must, that is called fraud. That is also a crime, and is covered by paragraph 2(1)(a).

Victoria Atkins: I take the right hon. Gentleman’s point, particularly in relation to the overstayer, but as the purpose of processing personal data in many immigration areas is not generally the pursuit of criminal enforcement action, it is not clear that it would be appropriate in all cases to rely on crime-related exemptions, where the real prejudice lies in our ability to take administrative enforcement action. It may well be that in some cases a crime has been committed, but that will not always be the case.

Criminal sanctions are not always the correct and proportionate response to people who are in the UK without lawful authority. It is often better to use administrative means to remove such a person and prevent re-entry, rather than to deploy the fully panoply of the criminal justice system, which is designed to rehabilitate members of our communities. As the purpose
of processing personal data in such cases is not generally the pursuit of a prosecution, it is not clear that we could, in all cases, rely on that exemption relating to crime.

Stuart C. McDonald: So far we have had some hypothetical examples about what might happen in the future, but given that we have a data protection regime in place already, it would be useful to know whether the Minister can give us examples of situations that have arisen in which the Home Office has been hindered by the current data protection regime. We have not heard anything like that so far.

Victoria Atkins: If I may, I will continue with my speech, because I have more information to give. Perhaps at the end I can deal with the hon. Gentleman’s point.

Liam Byrne: I just want to dissolve one confusion in the Minister’s remarks. The nature of the Home Office response, whether it is a prosecution through a civil court, a civil sanction or a civil whatever else, does not affect the nature of the offence that is committed. The Home Office has a range of sanctions and choices in responding to an offence, but that does not stop the offence being an offence. The offence is still a crime, and is therefore covered by paragraph 2(1)(a).

Victoria Atkins: The right hon. Gentleman is assuming that each and every immigration case that will be covered by these provisions necessitates the commission of a crime.

Liam Byrne: We are preventing crime.

Victoria Atkins: I would not make that assumption. The vast majority of immigration cases are dealt with in a civil context.

Darren Jones: Will the Minister give way?

Victoria Atkins: No, forgive me. I have been very generous with interventions. I am going to make some progress, and then no doubt others will intervene on me in due course.

I turn to the charge that the exemption has no basis in EU law. Article 23 of the GDPR allows member states to restrict the application of certain provisions of the regulation to safeguard important objectives of general public interest. Immigration control constitutes one such objective. We see immigration as an important matter of public interest, and the GDPR allows member states to exempt rights where that is the case. We are not alone in our belief that immigration is an important matter of general public interest. The Irish Government clearly stated that in their own Data Protection Bill. Clause 54 of the Irish Bill gives powers to make regulations restricting certain rights and obligations under the GDPR to safeguard important objectives of general public interest. The list of such objectives in the Bill includes matters relating to immigration.

Opposition Members have talked about their concerns about the fact that these provisions may be covered by paragraph 2 of the schedule. I want to reflect on the outcome of the debate on this provision in the House of Lords, which contains many noble Lords who are extremely learned in the law, have much experience of campaigning on immigration rights and so on. We listened very carefully to the concerns raised at Lords Committee stage, and as a result the Government tabled amendments at Lords Report stage to narrow the scope of the exemption so that it no longer covers the right to rectification and data portability. In response to those amendments, Lord Kennedy of Southwark said:

“The amendments tabled by the Government provide important clarification on what is exempt, limit the power in Bill and seek to address the concerns highlighted during the previous debate and today...I am happy to support their amendments.”—[Official Report, House of Lords, 13 December 2017; Vol. 787, c. 1590.]

Furthermore, in a Division on a Liberal Democrat amendment to strike out the immigration exemption, the official Opposition abstained. I wonder what has changed between their abstaining on that amendment and accepting that the Government’s amendments were sufficient, and today. Nothing has changed since the Bill left the Lords, so perhaps the right hon. Member for Birmingham, Hodge Hill can help us with why their position has changed.

I hope I have been able to satisfy the Committee that this provision is necessary and important.

Gareth Snell (Stoke-on-Trent Central) (Lab/Co-op): It is a pleasure to serve under your chairmanship, Mr Hanson. Will the Minister give a tangible example, as she has done in other cases, of where an immigration case may require exemption under paragraph 4—in other words, a case in which a crime has not been committed and therefore would not be covered under paragraph 2(2)? The cases she has mentioned so far would, on the face of it, be covered by paragraph 2(2), because a criminal act had taken place or was about to take place.

Victoria Atkins: There may be occasions when there is a person we have lost track of whose status is irregular. If we know they have a child, we will seek from the Department for Education assistance to find the whereabouts of the child. That child has not committed a criminal offence, so I would be very concerned to ensure that the Home Office, Border Force or whoever else acted lawfully when seeking that data in order to enable them to find the parent or whoever is the responsible adult, as part of the immigration system.

Louise Haigh: In that example, would the exemption not be covered under the safeguarding exemption, as brought by the Government amendment to schedule 1?

Victoria Atkins: I have to say, that had not occurred to me as an obvious—

Louise Haigh: A missing child?

Victoria Atkins: No—the child is not missing, but the parent is; so we seek advice from the Department for Education about where the child is. It may be that cleverer lawyers than me in the Home Office will find an exemption for that, but the point of this exemption of paragraph 4 is to cover the lawfulness of the Home Office in seeking such information in order to find parents or responsible adults who may have responsibility, and either to regularise their stay or to remove them.

I encourage the right hon. Member for Birmingham, Hodge Hill to withdraw his amendment, as we believe that it is not the wholesale disapplication of data subjects’
rights, and it is a targeted provision wholly in accordance with the discretion afforded to member states by the GDPR and is vital to maintaining the integrity and effectiveness of our immigration system.

**Liam Byrne:** Anyone who was not alarmed by this provision certainly will leave this Committee Room thoroughly alarmed by the Minister’s explanations.

First, we were invited to believe that we could safeguard due process and the rights of newcomers to this country by suspending those rights and pursuing people through civil court. We were then asked to believe that the Home Office’s ambition to deal with these cases with civil response rendered inoperable the powers set out in paragraph 2(1)(a), confusing the response from the Home Office and the nature of the offence committed up front. Then, we were invited to believe that this was not a permanent provision—even though that safeguard is not written into the Bill—but a temporary provision. What is not clear is when those temporary provisions would be activated and, crucially, when they would be suspended.

**Victoria Atkins:**

**Liam Byrne:** I am happy to give way in a moment. Most of us here who have done our fair share of immigration cases—I have done several thousand over the last 14 years—know that on some occasions, the Home Office interpretation of time is somewhat different from a broadly understood interpretation of time. I have cases in which a judge has ordered the issue of a visa, and six months later we are still chasing the Home Office for the issue of the visa. I will not be alone in offering these examples.

Perhaps when the Minister intervenes, she could set out what “temporary” means, where it is defined and where are the limits, and she still has not answered my question whether she will guarantee that the implementation of this pause will not jeopardise someone’s ability to submit either a request for an entry clearance officer review or an appeal within the legally binding time windows set out in Home Office regulations.

**Victoria Atkins:** The key to this is the purpose for which we are processing the data. Even if there are criminal sanctions, that does not mean that we are processing for that purpose, particularly where we are not likely to pursue a prosecution. The primary purpose is often immigration control—that does not fit under paragraph 2 as he has described it—rather than enforcing the criminal justice system. That is the point. It is for the purpose of processing the data. The crime-related provisions in the Bill refer to the importance of identifying the purposes of the processing. Where the primary purpose is immigration related, it is not clear that we could rely on the crime-related exemptions. That is why paragraph 4 is in the schedule.

**Liam Byrne:** I am really sorry to have to say this, but that is utter nonsense. The idea that the Home Office will seek to regularise someone’s immigration status by denying them access to information that might support their case is, frankly, fanciful.

This is not a new debate; we last had it in 1983. The Home Office tried to sketch this exemption into legislation then, it failed, and we should not allow the exemption to go into the Bill, especially given that all the explanations we have heard this afternoon are about cases where paragraph 2(1)(a), or the safeguarding provisions drafted by the Government, would provide the necessary exemptions and safeguards in the contingencies that the Minister is concerned about.

4.15 pm

**Darren Jones:** I feel for the Under-Secretary, because she is on a bit of a sticky wicket given the Government’s drafting, but does my right hon. Friend agree that it is concerning that I asked twice to be pointed to specifics—I asked first how the pause is drafted in the Bill, and secondly where the word “immigration” appears under article 23 of the GDPR—but on neither occasion was I pointed to them? We ought also to draw the Committee’s attention to the report on the Bill by the Joint Committee on Human Rights, which states:

“The GDPR does not expressly provide for immigration control as a legitimate ground for exemption.”

**Liam Byrne:** My hon. Friend is bang on the money, but perhaps the Under-Secretary can enlighten us.

**Victoria Atkins:** All rights are reinstated once the risk to prejudice is removed. The wording is in line 35 of paragraph 4:

“to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) and (b).”

To reassure the hon. Member for Bristol North West, that is the end point.

**Liam Byrne:** I am grateful to the Under-Secretary for clarifying a point that was not at issue. No one is concerned about what rights kick back in at the end of a process. We are worried about how long the process will last, who will govern it, what rights newcomers to this country or courts will have to enforce some kind of constraint on the process and how we will stop the Home Office embarking on unending processes in a Jarndyce v. Jarndyce-like way, which we know is the way these cases are sometimes prosecuted. The Home Office is full of some of the most amazing civil servants on earth, but perhaps, a little like the Under-Secretary, they are sometimes good people trapped in bad systems and, dare I say it, bad arguments.

**Question put.** That the amendment be made.

**The Committee divided:** Ayes 9, Noes 10.

**Division No. 4**

**AYES**

Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren
McDonald, Stuart C.

**NOES**

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

Murray, Ian
O’Hara, Brendan
Snell, Gareth
Zeichner, Daniel
Jack, Mr Alister
James, Margot
Lopez, Julia
Warman, Matt
Wood, Mike
Amendments made: 95, in schedule 2, page 138, line 15, at end insert—

“( 1 ) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);”

This amendment adds Article 19 of the GDPR (notification obligation regarding rectification or erasure of personal data or restriction of processing) to the list of GDPR provisions that are disapplied by provisions in Part 2 of Schedule 2 to the Bill.

Amendment 96, in schedule 2, page 139, leave out lines 17 to 27 and insert—

“2. The function is designed to protect members of the public against—

(a) dishonesty, malpractice or other seriously improper conduct, or

(b) unfitness or incompetence.

This amendment extends the exemption provided for in paragraph 6 of Schedule 2. It amends the second entry in the table (functions designed to protect members of the public against dishonesty etc) by removing the requirement that the function relates to people who carry on activities which bring them into contact with members of the public. It also amends column 2 of the table to bring the second entry into line with the first and third entries.

Amendment 97, in schedule 2, page 140, line 42, at end insert—

“Audit functions

7A (1) The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a function listed in sub-paragraph (2) to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

(2) The functions are any function that is conferred by an enactment on—

(a) the Comptroller and Auditor General;

(b) the Auditor General for Scotland;

(c) the Auditor General for Wales;

(d) the Comptroller and Auditor General for Northern Ireland.

This amendment inserts a new paragraph into Schedule 2 to provide for an exemption from “the listed GDPR provisions” (defined in paragraph 6 of Schedule 2) where personal data is processed for the purposes of discharging statutory functions of certain auditors.

Amendment 98, in schedule 2, page 140, line 42, at end insert—

“Functions of the Bank of England

7B (1) The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a relevant function of the Bank of England to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

(2) ‘Relevant function of the Bank of England’ means—

(a) a function discharged by the Bank acting in its capacity as a monetary authority (as defined in section 244(2)(c) and (2A) of the Banking Act 2009);

(b) a public function of the Bank within the meaning of section 349 of the Financial Services and Markets Act 2000;

(c) a function conferred on the Prudential Regulation Authority by or under the Financial Services and Markets Act 2000 or by another enactment.

This amendment inserts a new paragraph into Schedule 2 to provide for an exemption from “the listed GDPR provisions” (defined in paragraph 6 of Schedule 2) where personal data is processed for the purposes of discharging specified functions of the Bank of England.
and insert “when”.

This amendment is consequential on Amendment 71.

Amendment 108, in schedule 2, page 149, line 25, leave out “the date of”.

This amendment is consequential on Amendment 71.

Amendment 109, in schedule 2, page 150, line 45, at end insert—

“( ) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);”

This amendment adds Article 19 of the GDPR (notification obligation regarding rectification or erasure of personal data or restriction of processing) to the list of GDPR provisions that are disapplied by paragraph 24 of Schedule 2 to the Bill (journalistic, academic, artistic and literary purposes).

Amendment 110, in schedule 2, page 151, line 1, after “processor)” insert “—

(i) Article 34(1) and (4) (communication of personal data breach to the data subject);

(ii) “—(Margot James.)

This amendment adds Article 34 of the GDPR (communication of personal data breach to the data subject) to the list of GDPR provisions that are disapplied by paragraph 24 of Schedule 2 to the Bill (journalistic, academic, artistic and literary purposes).

Liam Byrne: I beg to move amendment 170, in schedule 2, page 151, line 8, at end insert—

“(f) in Chapter IX of the GDPR (provisions relating to research purposes or statistical purposes).”

This amendment adds the restrictions imposed on archiving by the GDPR and the Bill to the list of matters in the Bill that benefit from the Journalism, Art and Literature exemption.

The purpose of this amendment is to protect some of our important national archives. We in this country are some of the greatest collectors on earth; the tradition established by Sir Hans Sloane all those centuries ago inspired many generations that followed him. Our ability and our tradition of collecting mean that this country is now home to some of the greatest collections on the planet.

It is fantastic to see many of these institutions now rapidly digitalising those archives. I was privileged to be able to visit the Natural History Museum recently, which I think is home to something like 83 million different specimens. It is now beginning to digitalise those archives in a way that opens them up not only to our schoolchildren, but to citizens of this country and those around the world who are keen on science.

The point of this amendment is that we cannot simply preserve those archives in aspic. They must be dynamic resources; they must be added to, and our success or failure in that task has a crucial bearing on the health of our democracy and our ability to, dare I say it, reflect on past mistakes and do better. I think it was the legendary Karl Popper who once said, “To err is human, to correct divine.”

We make mistakes. It is important that we reflect on the mistakes we have made in the past, in order to do better next time around. Many of the more contemporary archives, particularly news archives, have had a crucial bearing on inquiries into historical child abuse, the injustices perpetrated at Hillsborough and at Orgreave, and HIV-contaminated blood. All those inquiries relied on records that were not necessarily historical; many were contemporary.

A range of crucial organisations entrusted with the delicate task of keeping our archives up to date are seriously worried about the provisions in the GDPR. In fact, they believe the inadequacy of the derogations and exemptions in the GDPR, as it is proposed that we draft it into law, means that they will be quickly put out of business. In particular, that will bite on thousands of smaller archives.

The point they have consistently made to us is that, although we have such great collections and archives in this country and a public interest culture around protecting some of those archives, we do not have any of the kind of legal protections that they enjoy in countries such as France. We do not have the defensible protections around archives that those abroad benefit from.

The challenge in this Bill is a lack of precision. I do not want to pretend that this is a black-and-white case. Sometimes news archives in particular will be required to draw something of a grey line, and I am afraid the Minister has to earn her pay and be the one to decide where to draw that grey line. Sometimes there will be information stored in those archives that absolutely should be subject to the GDPR provisions. But if we are in effect granting a carte blanche for people to make requests of archives that require those archives to dip deep into the historical record, correct things and go through challenging processes to ensure they are right, I am afraid it will put a number of our archives out of business, and that will damage the health of our democracy.

We have drafted this amendment with a number of aims. We want to try to create a statutory definition for organisations that archive in the public interest. We have had a first attempt at drawing that in a narrow way, so it does not infringe on material that is stored that absolutely should be subject to general GDPR provisions. We have done our best to ensure that the archiving exemptions are proportionate to the public interest nature of the material being archived. We wanted to offer an amendment worded hopefully in such a way that, frankly, it excludes Google, Facebook and others from enjoying the exemptions sought here.

This is the first place in the Bill where the debate rears its head. I am grateful to the range of museums, archives and the BBC that have helped us to craft this amendment. It should not be particularly controversial. There should be agreement across the Committee on the need to protect our great collections, yet keep some companies, such as Google and Facebook, subject to the provisions in the Bill.

We offer the amendment as a starter for 10. Obviously, we would be delighted if the Government accepted it; we would be even more pleased if they could perfect it.

The Chair: I have just had a request to remove jackets, because of the warm temperature in the room. I give my permission to do so. I call the Minister.

Margot James: Thank you, Mr Hanson. I agree with the tribute paid by the right hon. Member for Birmingham, Hodge Hill to the custodians of some of the most wonderful archives in the world. I will comment on his proposals with regard to such archives shortly, but I hope that recent debates have left no doubt in
hon. Members' minds that the Government are absolutely committed to preserving the freedom of the press, and maintaining the balance between privacy and freedom of expression in our existing law, which has served us well for so many years.

As set out in the Bill, media organisations can already process data for journalistic purposes, which includes media archiving. As such, we believe that amendment 170 is unnecessary and could be unhelpful. I agree with the right hon. Gentleman that it is crucial that the media can process data and maintain media archives. In the House of Lords, my noble Friend Lord Black of Brentwood explained very well the value of media archives. He said:

“Those records are not just the ‘first draft of history’; they often now comprise the only record of significant events, which will be essential to historians and others in future, and they must be protected.”—[Official Report, House of Lords, 10 October 2017; Vol. 785, c. 175.]

However, recital 153 indicates that processing for special purposes includes news archiving and press libraries. Paragraph 24 of schedule 2 sets out the range of derogations that apply to processing for journalistic purposes. That includes, for example, exemption from complying with requests for the right to be forgotten. That means that where the exemption applies, data subjects would not have grounds to request that data about them be deleted. It is irrelevant whether the data causes substantial damage or distress.

However, if media organisations are archiving data for other purposes—for example, in connection with subscriber data—it is only right that they are subjected to the safeguards set out in article 89(1), and the Bill provides for that accordingly. For that reason, I hope that the right hon. Gentleman agrees to reconsider his approach and withdraw his amendment.

**Liam Byrne:** I am happy to withdraw the amendment, although I would say to the Minister that the helpful words we have heard this afternoon will not go far enough to satisfy the objections that we heard from organisations. We reserve the right to come back to this matter on Report. We will obviously consult the organisations that helped us to draft the amendment, and I urge her to do the same. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Schedule 2, as amended, agreed to.

**Schedule 3**

**EXEMPTIONS ETC FROM THE GDPR: HEALTH, SOCIAL WORK, EDUCATION AND CHILD ABUSE DATA**

**Amendments made:** 111, in schedule 3, page 160, line 21, leave out “with the day on which” and insert “when”.

This amendment is consequential on Amendment 71.

Amendment 112, in schedule 3, page 162, line 3, leave out paragraph 16 and insert—

“16 (1) This paragraph applies to a record of information which—

(a) is processed by or on behalf of the Board of Governors, proprietor or trustees of, or a teacher at, a school in Northern Ireland specified in sub-paragraph (3),

(b) relates to an individual who is or has been a pupil at the school, and

(c) originated from, or was supplied by or on behalf of, any of the persons specified in sub-paragraph (4).

(2) But this paragraph does not apply to information which is processed by a teacher solely for the teacher’s own use.

(3) The schools referred to in sub-paragraph (1)(a) are—

(a) a grant-aided school;

(b) an independent school.

(4) The persons referred to in sub-paragraph (1)(c) are—

(a) a teacher at the school;

(b) an employee of the Education Authority, other than a teacher at the school;

(c) an employee of the Council for Catholic Maintained Schools, other than a teacher at the school;

(d) the pupil to whom the record relates;

(e) a parent, as defined by Article 2(2) of the Education and Libraries (Northern Ireland) Order 1986 (S.I. 1986/594 (N.I. 3)).

(5) In this paragraph, “grant-aided school”, “independent school”, “proprietor” and “trustees” have the same meaning as in the Education and Libraries (Northern Ireland) Order 1986 (S.I. 1986/594 (N.I. 3)).”

This amendment expands the types of records that are “educational records” for the purposes of Part 4 of Schedule 3.

Amendment 113, in schedule 3, page 164, line 7, leave out “with the day on which” and insert “when”.—[Margot James.]

This amendment is consequential on Amendment 71.

Schedule 3, as amended, agreed to.

Schedule 4 agreed to.

**Clause 16**

**POWER TO MAKE FURTHER EXEMPTIONS ETC BY REGULATIONS**

**Question proposed,** That the clause stand part of the Bill.

4.30 pm

**Stuart C. McDonald:** This morning we had a discussion about some of the Henry VIII clauses contained in the Bill. In essence, I said that when we are talking about personal information—particularly, in such circumstances, sensitive personal information—there should be a strong presumption against Henry VIII clauses, with the onus being on the Government to justify why delegated legislation is the appropriate way to make changes to our data protection rules.

Throughout the passage of the Bill we will continue to challenge the Government to justify delegated powers proposed under the Bill. This clause is the next example of that arising, so in our view it falls on the Minister to explain why she seeks delegated authority to exercise certain functions under the GDPR. I look forward to hearing what she has to say.

**Liam Byrne:** We agree that the clause offers Ministers a rather sweeping power to introduce new regulations. Over the course of what has been quite a short day in Committee we have heard many reasons to be alarmed about equipping Ministers with such sweeping powers. We proposed an amendment to remove the clause, which I think was not selected because we have this stand part debate. What we need to hear from the
Minister are some pretty good arguments as to why Ministers should be given unfettered power to introduce such regulations without the effective scrutiny and oversight of right hon. and hon. Members in this House.

**Margot James:** I am glad that the right hon. Gentleman feels we have had a short day in Committee. In answer to his questions and those of the hon. Gentleman, the order making powers in clauses 16 and 113 allow the Secretary of State to keep the list of exemptions in schedules 2 to 4 and 11 up to date. As I mentioned when we discussed order making powers in relation to clause 10 and schedule 1, we carefully reviewed the use of such powers in the Bill following recommendations from the Delegated Powers and Regulatory Reform Committee. We think an appropriate balance has now been struck. It might be helpful if I explain the reasons for our thinking.

Clause 16 includes order making powers to ensure that the Secretary of State can update from time to time the particular circumstances in which data subjects' rights can be disapplied. That might be necessary if, for example, the functions of a regulator are expanded and exemptions are required to ensure that those new functions cannot be prejudiced by a data subject exercising his or her right to object to the processing.

We believe it is very important that the power to update the schedules is retained. Several of the provisions in schedules 2 to 4 did not appear in the Data Protection Act 1998 and have been added to the Bill to address specific requirements that have arisen over the last 20 years.

For example, the regulatory landscape has changed dramatically since the 1998 Act. Organisations such as the Bank of England, the Financial Conduct Authority and the National Audit Office have taken on a far broader range of regulatory functions, and that is reflected in the various amendments we have tabled to paragraphs 7 to 9 of schedule 2, to provide for a broader range of exemptions. No doubt, there will be further changes to the regulatory landscape in the years to come. Of course, other exemptions in schedule 2 have been carried over from the 1998 Act, or indeed from secondary legislation made under that Act, with little change. That does not mean, however, that they will never need to be amended in the future. Provisions made under the 1998 Act could be amended via secondary legislation, so it would seem remiss not to afford ourselves that same degree of flexibility now. If we have to wait for primary legislation to make any changes, it could result in a delay of months or possibly years to narrow or widen an extension, even where a clear deficiency had been identified. We cannot predict the future, and it is important that we retain the power to update the schedules quickly when the need arises.

Importantly, any regulations made under either clause would be subject to the affirmative resolution procedure. There would be considerable parliamentary oversight before any changes could be made using these powers. Clause 179 requires the Secretary of State to consult with the Information Commissioner and other interested parties that he considers appropriate before any changes are made.

I hope that that reassures Members that we have considered the issue carefully. I commend clause 16 to the Committee.

**Question put,** That the clause stand part of the Bill. **The Committee proceeded to a Division.**

The Chair: The ayes were 10, the noes were nine. No—[Interuption.] I have been here a long time.

The Committee having divided: Ayes 10, Noes 9.

**Division No. 5**

**AYES**

Adams, Nigel  
Atkins, Victoria  
Clark, Colin  
Heaton-Jones, Peter  
Huddleston, Nigel

**NOES**

Byrne, rh Liam  
Elmore, Chris  
Haigh, Louise  
Jones, Darren  
McDonald, Stuart C.

Question accordingly agreed to.

Clause 16 ordered to stand part of the Bill.

**Clause 17**

**ACCREDITATION OF CERTIFICATION PROVIDERS**

Margot James: I beg to move amendment 15, in clause 17, page 10, line 16, leave out “authority” and insert “body”.

This amendment corrects the reference in Clause 17(7) to the “national accreditation authority” by amending it to refer to the “national accreditation body”, which is defined in Clause 17(8).

Clause 17 relates to the certification of data controllers. This is a relatively new concept and will take time to bed in, but it could also be a significant step forward in ensuring that data subjects can have confidence in controllers and processors and, perhaps even more important, that controllers and processors can have confidence in each other. It is likely to be particularly relevant in the context of cloud computing and other business-to-business platforms where individual audits are often not feasible in practice.

Before they can audit controllers, certification bodies must be accredited, either by the Information Commissioner or by the national accreditation body, UKAS. Clause 17 and schedule 5 set out how the process will be managed. Unfortunately, there is a typographical error in clause 17. It refers erroneously to the “national accreditation authority” in subsection (7), when it should refer to the “national accreditation body”. Amendment 15 corrects that error.

Amendment 15 agreed to.

Clause 17, as amended, ordered to stand part of the Bill.

**Schedule 5**

**ACCREDITATION OF CERTIFICATION PROVIDERS: REVIEWS AND APPEALS**

Amendment made: 114, in schedule 5, page 170, line 21, leave out “In this paragraph” and insert—

“Meaning of “working day””

7 In this Schedule”
This amendment applies the definition of “working day” for the purposes of the whole of Schedule 5. There are references to “working days” in paragraphs 5(2) and 6(3) of that Schedule.—(Margot James.)

Schedule 5, as amended, agreed to.

Clause 18 ordered to stand part of the Bill.

Clause 19

Processing for Archiving, Research and Statistical Purposes: Safeguards

Amendment made: 16, in clause 19, page 12, line 2, leave out “(d)” and insert “(e)” — (Margot James.)

This amendment amends the definition of “relevant NHS body” in this Clause by adding special health and social care agencies established under Article 3 of the Health and Personal Social Services (Special Agencies) (Northern Ireland) Order 1990 (which fall within paragraph (e) of section 1(5) of the Health and Social Care (Reform) Act (Northern Ireland) 2009).

Clause 19, as amended, ordered to stand part of the Bill.

Clauses 20 to 22 ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned.—(Nigel Adams.)

4.43 pm

Adjourned till Thursday 15 March at half-past Eleven o’clock.
Written evidence reported to the House

DPB 01 David Burns
DPB 02 Liberty
DPB 03 Michael Veale UCL, Dr Reuben Binns U Oxford, Prof Lilian Edwards U (Strathclyde)
DPB 04 Future Care Capital
DPB 05 Information Commissioner’s Office
DPB 06 Big Brother Watch
DPB 07 Privacy International
DPB 08 Stephen Rickitt, Clerk to Glanton, Meldon, Milfield, Mitford and Whalton Parish Councils
DPB 09 British Dental Association
DPB 10 Optical Confederation
DPB 11 Press Association

DPB 12 WAN-IFRA, CPU Media Trust, and News Media Europe
DPB 13 Sport and Recreation Alliance
DPB 14 BMA (British Medical Association)
DPB 15 John Gordon
DPB 16 Immigration Law Practitioners’ Association (ILPA)
DPB 17 British Paraolympic Association
DPB 18 YoungMinds and The Children’s Society
DPB 19 Pact
DPB 20 The Law Society
DPB 21 The Officers’ Association
DPB 22 Amnesty International UK
DPB 23 Association for Financial Markets in Europe (AFME)
DPB 24 News Media Association
CONTENTS

SCHEDULE 6 agreed to, with an amendment.

CLauses 23 to 26 agreed to, one with an amendment.

Clause 27 under consideration when the Committee adjourned till this day at Two o'clock.
No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Monday 19 March 2018
The Committee consisted of the following Members:

Chairs: David Hanson, Mr Gary Streeter

† Adams, Nigel (Lord Commissioner of Her Majesty’s Treasury)
† Atkins, Victoria (Parliamentary Under-Secretary of State for the Home Department)
† Byrne, Liam (Birmingham, Hodge Hill) (Lab)
† Clark, Colin (Gordon) (Con)
† Elmore, Chris (Ogmore) (Lab)
† Haigh, Louise (Sheffield, Heeley) (Lab)
† Heaton-Jones, Peter (North Devon) (Con)
† Huddleston, Nigel (Mid Worcestershire) (Con)
† Jack, Mr Alister (Dumfries and Galloway) (Con)
† James, Margot (Minister of State, Department for Digital, Culture, Media and Sport)

† Jones, Darren (Bristol North West) (Lab)
† Lopez, Julia (Hornchurch and Upminster) (Con)
† McDonald, Stuart C. (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP)
† Murray, Ian (Edinburgh South) (Lab)
† O’Hara, Brendan (Argyll and Bute) (SNP)
† Snell, Gareth (Stoke-on-Trent Central) (Lab/Co-op)
† Warman, Matt (Boston and Skegness) (Con)
† Wood, Mike (Dudley South) (Con)
† Zeichner, Daniel (Cambridge) (Lab)

Kenneth Fox, Committee Clerk

† attended the Committee
Tuesday, would assist the Government in securing a finding of adequacy from the European Commission so that, if the UK leaves the European Union, we can continue to exchange data with it. As the Committee knows, I like to refer to my version of the general data protection regulation as much as to the Bill, even though it is not the subject of our debate today.

I welcome the Government’s commitments on the Floor of the House to seeking something “akin to” adequacy, then adequacy, and then something “beyond adequacy”. I thank the Minister, the hon. Member for Stourbridge, for her response to my question on Second Reading about wanting “beyond adequacy” to represent a useful position for our Information Commissioner on the European data protection board. Some of us have concerns about that because of the practicalities of what happens with third countries. Indeed, I asked the Information Commissioner herself about it at an evidence session of the Select Committee on Science and Technology, and she confirmed that third countries traditionally have little influence on the article 29 working party—the predecessor of the EDPB—even if they have a seat at the table.

I think our shared view is that in seeking “beyond adequacy”, we want not only to have a seat at the table as a potential third country but to have influence. In order to have that influence, we need to go slightly above and beyond what other third countries do and show close co-operation between the UK and the European Union.

Article 45 of the GDPR sets out guidelines on how the European Commission will assess and agree decisions on adequacy. It has to be happy that our legal framework is in line with its own. Of course, there will be an initial conversation as part of trade negotiations with the European Union. Under paragraph 3, the Commission is then to undertake “a periodic review, at least every four years” to ensure that we continue to be compliant. Paragraph 4 refers to ongoing monitoring of developments in third countries in their application of data protection laws and privacy rights.

As I have said on Second Reading and in previous debates on data protection laws, my concern is that we should lockstep the developments in our legislation, guidance and codes of conduct to show that they are still in line with the leading European Union legislative framework for data protection, so that we can continue to flow important amounts of data. Some 70% of our data flow is with the EU, and the UK accounts for a huge proportion—around 11%—of global data flow. We must maintain that. Under article 30 of the GDPR, in deciding on adequacy, the European Commission must seek “mechanisms to facilitate the effective enforcement of legislation”.

This is our opportunity to show the European Union that we are committed to data protection principles. Amendment 152 would tweak the wording of paragraph 2 of article 61 of the applied GDPR. I was pleased to see that paragraph; in earlier debates I raised some concerns that—for political reasons that I will not go into today—the Bill might not go as far as admitting that we need to track and implement EU law in the area. However, I want to strengthen the paragraph 2 wording, which says that our Information Commissioner must “have regard to” various things that happen at European Union level, including “decisions, advice, guidelines, recommendations and best practices issued by the European Data Protection Board”.

The amendment seeks to strengthen that slightly, while recognising that the Government, and probably also the Information Commissioner, would like a little flexibility.

Liam Byrne (Birmingham, Hodge Hill) (Lab): This is a wise and carefully crafted amendment. Does my hon. Friend agree that it is especially needed because the Government have rather unwisely decided not to incorporate article 8 into British law, which means there is a risk of courts in Europe and Britain interpreting data protection regimes differently, leading to divergence in future?

Darren Jones: I agree. I am attempting not to get too much into the party politics in a bid to seek the Government’s agreement to the amendment, but there is an important distinction to be made. We have a layering of risks in seeking to achieve adequacy. On Tuesday we debated at length the Government’s decision to repeal fundamental rights of the European charter, which we know from European guidelines is something they look to. We will come to issues of national security today, which is also an issue for third countries, as we have seen with Canada.

This small amendment would help mitigate some of that risk by making it clear to our friends in the European Union that we in Britain are proud about the influence we had in drafting the general data protection regulation, which is a world-leading set of laws and rules for the
future of our digital economy, and we continue to want to play a part in that, to help lead the conversation in the world and at European Union level. In co-operation with our friends in Europe, we seek to maintain that. While the Government may wish for divergence in other areas, I take the view that they do not in this area because we have been at the forefront of developments.

The amendment seeks only to tweak what is already in the Bill. As Members will see, it says that we would “incorporate, with any modifications which he or she”—that is the Information Commissioner—“considers necessary in any guidance or code of practice... decisions...issued by the European Data Protection Board”. There is a nuanced difference; the Bill as drafted speaks of having “regard to”, while the amendment speaks of incorporating, with any modifications that the Information Commissioner feels fit. It may seem like I am getting stuck in semantics— I do quite like to do that—but the amendment would deliver an important tone to the European Commission. On passing the Bill, we would be saying that when we are negotiating on data, where we have a shared interest at European and UK level, we want to get it right, and we will have gone beyond the basics of adequacy of other third countries because of our close relationship. We will hopefully have a seat on the European data protection board, where we seek to have influence, and we will take that responsibility seriously and, therefore, we will incorporate decisions of the board into the guidance of UK laws to lockstep our development in the area. As I said, it is made clear in the general data protection regulation that that is to be monitored on a continuous basis and more formally on a periodic basis.

I would not want us to lose adequacy in the future by diverging from European Union law. I want us to have an influential position on the European data protection board, which means being involved in the detail and taking the obligation of carrying that through on our side of the fence. The amendment seeks to bring that tone of co-operation and would help us and the Government in seeking adequacy so that we can secure these important data flows into the future.

Liam Byrne: It is a privilege to serve under your chairmanship, Mr Streeter. I rise to support my hon. Friend on his excellent, very helpful amendment. Earlier in the week we had a debate about the wisdom of incorporating article 8 into the Bill. I want to underline that we now have two different foundations for privacy that will operate post-Brexit in Europe and in the UK. The law is not fixed in aspect; it is a dynamic body of thought and ideas, and in the years to come there is a risk that courts in Europe and in the UK will diverge in how they interpret those fundamental principles.

That risk is all the more profound in this area of public policy because technology is moving so quickly. Therefore, if the Government wanted to do away with the risk to any future adequacy agreements, they would look for any and every opportunity to create bridges between the EU data protection regime and the British regime. The more bridges that are put in place, and the more girders that yoke us together in this field of public policy, the better.

Companies will consider whether regulatory harmonisation in data protection will continue when they make investment decisions in the technology space in the UK. I am afraid that that is now a fact of economic life. The simpler and faster the Government can help companies take those decisions, by putting beyond dispute and doubt any future adequacy agreement, the better. It is in our common interest to try to create stronger links than the Bill offers. I hope that the Government will accept the amendment.

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): It is a pleasure to serve under your chairmanship, Mr Streeter. I thank the hon. Member for Bristol North West, who has great knowledge of these issues and has put his thoughts on his amendment very well to the Committee. As the Prime Minister said in her Mansion House speech, the ability to transfer data across international borders is crucial to a well-functioning economy, and that will remain the case after we leave the European Union. We are committed to ensuring that uninterrupted data flows between the UK and the EU continue. One way we can help to ensure that we have the foundations for that relationship is to continue to apply our exceptionally high standards for the protection of personal data.

Amendment 152 relates to the applied GDPR, which exists to extend GDPR standards to personal data processed for purposes outside the scope of EU law that may be otherwise left unregulated. The amendment is to schedule 6 of the Bill, which creates the applied GDPR by modifying the text of the GDPR so that it makes sense for matters outside the scope of EU law. The extension of GDPR standards is vital, because having a complete data protection regulatory framework will provide the UK with a strong foundation from which to protect people’s personal data and secure the future free flow of data with the EU and the rest of the world. Applying consistent standards ensures that those bodies—mostly public authorities—who process personal data, both in and out of the scope of EU law, experience no discernible operational difference when doing so.

However, the applied GDPR, although very close, is not identical to the GDPR known as the real GDPR. The differences are primarily the inevitable result of extending text designed for the EU to matters over which the UK and other member states retain competence. Reference to member states becomes a reference to our country; reference to the supervisory authorities becomes a reference to the Information Commissioner, and so on. Similarly, the applied GDPR, as a purely domestic piece of regulation, is outside the scope of the functions of the European data protection board and the EU Commission.

Decisions and guidance issued by the European Data Protection Board will have an important bearing on the GDPR as implemented in the UK. To ensure that the interpretation of the applied element of the GDPR remains consistent with the interpretation of the real GDPR, it is right that the Information Commissioner should have regard to decisions and guidance issued by the European Data Protection Board in carrying out her functions, as the UK regulator and enforcer of the applied GDPR. However, the amendment goes further, by requiring her to incorporate them into her guidance and codes of practice. The effect of that is to extend the ambit of the European data protection board so that, uniquely among member states, it would have within its purview processing outside the scope of EU law, when that processing was undertaken in the UK.
We do not agree that such an extension is required for the UK to achieve the relationship that we are seeking. By contrast, the current requirement in paragraph 49 of the schedule, for the commissioner to have regard to decisions and guidance issued by the European Data Protection Board in carrying out her functions means that she can and, in some cases, should incorporate into her guidance what she recognises as relevant and necessary. We are confident that, founded on the commissioner’s discretion, remains the best approach. On that basis, I hope that the hon. Member for Bristol North West feels able to withdraw his amendment.

11.45 am

Daniel Zeichner (Cambridge) (Lab): It is a pleasure to serve under your chairmanship, Mr Street. I listened closely to the Minister—I am struggling with the real and the applied GDPRs, as I am sure we all are—and the sense I get is that that will lead to potential divergence, which could have further consequences. We have reached an important point in the discussion. If we have divergence a few years down the line, does that not put adequacy at risk?

Margot James: I reassure the hon. Gentleman. Gentleman that divergence, if it occurs, will apply only to the applied GDPR, which is outside the scope of EU law, and therefore may well apply in a similar sense to member states as well as to us, when we become a third country.

Darren Jones: I thank the Minister for her useful reply. She is right, of course, that the applied GDPR is different from the real GDPR. As I said, I am seeking to establish a beyond-adequacy outcome, which is the Government’s intention, according to their comments on Second Reading.

From other third countries, we know that adequacy decisions look at areas of non-EU competence—we will get into the detail of that later in the context of national security and the ongoing conversations with Canada; we already had a conversation on Tuesday about fundamental rights. Under the regulation, the European Commission has the power to look at the whole legislative environment in a third country, even where it is not an area of EU competence. That is an important point to be clear on.

The relationship may be unique compared with other third countries, but we are in a unique position as we leave the European Union. If we want to have strong, sustainable, ongoing adequacy, it is important that we take steps to establish that.

Liam Byrne: The Minister seemed to rest her argument on the need to preserve the Information Commissioner’s discretion, which implies that she is trying to protect the commissioner’s ability to go her own way. That will not help us to secure, lock down or nail to the floor an adequacy agreement in years to come. It will put an adequacy agreement at risk.

Darren Jones: My right hon. Friend is exactly right. Of course, the Information Commissioner is an excellent commissioner. We are privileged to have Elizabeth in the role here in the UK, not least with her experience, as a Canadian, of being in a third country. That is why I put some flexibility into my amendment—to recognise that situations may arise about which we cannot hypothesise today in which the commissioner will need some flexibility. Under my amendment, she has the power to add modifications that she considers necessary. The Government’s concerns about the lack of flexibility are not reflected in the drafting of my amendment, as I have tried to deal with that.

The idea that the amendment increases the European data protection board’s power is incorrect, because this is UK law, not European Union law. The amendment merely says that we will get only slightly further, with flexibility, by recognising that in the decisions that we want to be a part of—that is a really important point here—and to influence, we will take the obligations as well as the responsibilities, should we be invited to.

Daniel Zeichner: Could the Bill not also put the Information Commissioner in an extraordinarily difficult position? Decisions that she may make in the future could have huge political consequences. I would be surprised if she wanted to take that on.

Darren Jones: I agree with my hon. Friend. The reality may be that under the wording in the Bill, the Information Commissioner has no choice but to apply and incorporate the European data protection board’s decisions if it is to keep up and maintain adequacy.

That is why the amendment is not something to worry about. It seeks to do what will probably happen in practice, but it puts our commitment to that relationship in the Bill. When we say to Europe that, uniquely, unlike any other third country and despite not being a member of the European Union, we want to have a position of influence on the EDPB, we can also say that we recognise that no one else has that level of influence, but in seeking to have it, we have made commitments to that future relationship in UK legislation.

I do not think any other Members here are members of the European Scrutiny Committee, but I spent the whole of yesterday afternoon losing votes on amendments to a report, and I rather enjoyed myself, so I will press this amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 8, Noes 10.

Division No. 6]

AYES

Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren

McDonald, Stuart C.
Murray, Ian
O’Hara, Brendan
Zeichner, Daniel

NOES

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

Jack, Mr Alister
James, Margot
Lopez, Julia
Warmann, Matt
Wood, Mike

Question accordingly negatived.
Margot James: I beg to move amendment 115, in schedule 6, page 180, line 2, leave out sub-paragraph (b) and insert—

“(b) in paragraph 2, for ‘Member States’ substitute ‘The Secretary of State’;

(c) after that paragraph insert—

‘3 The power under paragraph 2 may only be exercised by making regulations under section (Duty to review provision for representation of data subjects) of the 2018 Act.’”

This amendment is consequential on NC2.

The Chair: With this it will be convenient to discuss the following:

Government amendments 63 to 68.

Amendment 154, in clause 183, page 106, line 24, at end insert—

“(4A) In accordance with Article 80(2) of the GDPR, a person who satisfies the conditions in Article 80(1) and who considers that the rights of a data subject under the GDPR have been infringed as a result of data processing, may bring proceedings, on behalf of the data subject and independently of the data subject’s mandate—

(a) pursuant to Article 77 (right to lodge a complaint with a supervisory authority),

(b) to exercise the rights referred to in Article 78 (right to an effective judicial remedy against a supervisory authority),

(c) to exercise the rights referred to in Article 79 (right to an effective judicial remedy against a controller or processor),

(4B) An individual who considers that rights under the GDPR, this Act or any other enactment relating to data protection have been infringed in respect of a class of individuals of which he or she forms part may bring proceedings in respect of the infringement as a representative of the class (individually of the mandate of other members of the class), and—

(a) for the purposes of this subsection ‘proceedings’ includes proceedings for damages, and any damages recovered are to be distributed or otherwise applied as directed by the court,

(b) in the case of a class consisting of or including children under the age of 18, an individual may bring proceedings as a representative of the class whether or not the individual’s own rights have been infringed,

(c) the court in which proceedings are brought may direct that the individual may not act as a representative, or may act as a representative only to a specified extent, for a specified purpose or subject to specified conditions,

(d) a direction under paragraph (c) may (subject to any direction of the court) be made on the application of a party or a member of the class, or of the court’s own motion, and

(e) subject to any direction of the court, a judgment or order given in proceedings in which a party is acting as a representative under this subsection is binding on all individuals represented in the proceedings, but may only be enforced by or against a person who is not a party to the proceedings with the permission of the court,

(4C) Subsections (4A) and (4B)—

(a) apply in respect of infringements occurring (or alleged to have occurred) whether before or after the commencement of this section,

(b) apply to proceedings begun before the commencement of this section as if references in subsections (4A) and (4B) to bringing proceedings included a reference to continuing proceedings, and

(c) are without prejudice to the generality of any other enactment or rule of law which permits the bringing of representative proceedings.”

This amendment would create a collective redress mechanism whereby a not-for-profit body, organisation or association can represent multiple individuals for infringement of their rights under the General Data Protection Regulation.

Amendment 155, in clause 205, page 120, line 38, at end insert—

“(ca) section 183 (4A) to (4C);”

This amendment would create a collective redress mechanism whereby a not-for-profit body, organisation or association can represent multiple individuals for infringement of their rights under the General Data Protection Regulation.

Government amendments 73 and 74.

Government new clause 1—Representation of data subjects with their authority: collective proceedings.

Government new clause 2—Duty to review provision for representation of data subjects.

Margot James: These Government amendments concern the issue of class representation for data protection breaches. Article 80(1) of the GDPR enables a not-for-profit organisation to represent a data subject on their behalf, if the data subject has mandated them to do so. The Bill gives effect to the same right in clause 183. Where a not-for-profit organisation wants to bring a claim on behalf of multiple people, as things stand it will need to make multiple applications to the court. That is not efficient, and it would be better if all the claims could be made in a single application.

New clause 1 gives the Secretary of State the power to set out provisions allowing a non-profit organisation to bring a claim on behalf of multiple data subjects under article 80(1). We have taken the practical view that that will be an effective way for a non-profit group to seek a remedy in the courts on behalf of a large number of data subjects. The Bill does not give effect to article 80(2), which allows not-for-profit bodies to represent individuals without their mandate. We believe that opt-out collective proceedings should be established on the basis of clear evidence of benefit, with a careful eye on the pitfalls that have befallen so-called class-action lawsuits in other jurisdictions. The Government have, however, listened to the concerns raised and accept that further consideration should be given to the merits of implementing the provisions in article 80(2).

New clause 2 provides a statutory requirement for the Secretary of State to conduct a review of the operation of article 80(1), which will consider how it and the associated provisions in the Bill have operated in practice and assess the merits of implementing article 80(2) in the future. The review will involve consultation among relevant stakeholders, such as the Information Commissioner, businesses, privacy groups, the courts, tribunals and other Departments. The new clause requires the Secretary of State to conduct the review and present its findings to Parliament within 30 months of the Bill’s coming into force. That is necessary to provide enough time for there to be sufficient evidence to scrutinise the options provided in article 80(1) in the civil courts. Were the review period to be substantially shorter, it would increase the likelihood of there being a paucity of evidence, which would undermine the effectiveness and purpose of the review. Upon the conclusion of the review period, the Secretary of State will have the
power, if warranted, to implement article 80(2), allowing non-profit organisations to exercise the rights awarded to data subjects under articles 77, 78, 79 and 82 on their behalf without first needing their authorisation to do so.

Amendments 63 to 68, 73, 74 and 115 are consequential amendments that tidy up the language of the related clause, clause 183. They provide additional information about the rights of data subjects that may be exercised by representative bodies. I commend the amendments to the Committee.

Liam Byrne: I will speak to amendments 154 and 155, which are in my name and those of my hon. Friends. The broad point I want to start with is a philosophical point about rights. If rights are to be real, two things need to be in place: first, a level of transparency so that we can see whether those rights are being honoured or breached; and, secondly, an efficient form of redress. If we do not have transparency and an effective, efficient and open means of redress, the rights are not real, so they are theoretical.

We think there are some unique circumstances in the field of data protection that require a slightly different approach from the one that the Government have proposed. The Government have basically proposed an opt-in approach with a review. We propose an opt-out approach. We think that the argument is clear cut, so we do not see why the Government have chosen to implement something of a half-measure.

The Bill gives us the opportunity to put in place an effective, efficient and world-leading form of redress to ensure that data protection rights are not breached. The reality is that large-scale data breaches are now part and parcel of life. They affect not only the private sector but the private sector, which is partnering with Government. We have seen a number of data breaches among Government partners where financial information has been leaked. The reality is that data protection breaches around the world are growing in number and size.

What is particularly egregious is that many private sector companies admit to the scale of a data breach only many years after the offence has taken place. Yahoo! is a case in point. It had one of the biggest data breaches so far known, but it took many months before the truth came out. That has been true of Government partners, too. Sometimes a lesser offence is admitted to. There is muttering about a particular problem and then, as the truth unfolds, we hear that a massive data breach has taken place. The reality is that these firms are by and large going unpunished. Although the Bill proposes some new remedies of a significant scale, unless those remedies can be sought by ordinary citizens in a court, they frankly are not worth the paper they are printed on.

To underline that point, I remind the Committee that often we look to the Information Commissioner to take the lead in prosecuting these offences. My hon. Friend the Member for Bristol North West was right to celebrate the strength of our current Information Commissioner, but the Government have not blessed the Information Commissioner with unlimited resources, and that will not change in the foreseeable future. What that means is that in the last year for which we have information—2016-17—the Information Commissioner issued only 16 civil monetary penalties for data breaches. That is a very small number. We think we need a regime that allows citizens to bring actions in court. That would multiply the power of the Information Commissioner.

Article 80 of the GDPR addresses that problem in a couple of ways, and the Minister has alluded to them. Article 81 basically allows group or class actions to be taken, and article 82 says that the national law can allow representative bodies to bring proceedings. The challenge with the way in which the Government propose to activate that power is that the organisation bringing the class action must seek a positive authorisation and people must opt in. The risk is that that will create a burden so large that many organisations will simply not step up to the task.

12 noon

A world-leading charity and consumer rights organisation such as Which?, for example, would have a board of trustees to which it would be accountable. It would have to satisfy the trustees that it was not about to embark on something very difficult and expensive. I think most trustees would regard bringing a class action against Google, Facebook, Apple or Microsoft as a reasonably high risk action. If they then have to get a positive opt-in from a large number of people, like the 100,000 affected by the Morrisons data breach, it simply will not happen.

The mechanism that the Government propose breaks down in two particular ways in the real world. First, it takes no account of the gigantic asymmetry between the fearsome five data giants, or indeed many of the other large organisations that control tons and tons of our data, and the humble individual. I mentioned earlier in our proceedings that the big five data giants have a combined market capitalisation of $2.4 trillion. They have billions and billions in cash sitting on their balance sheets. Their legal power is practically unlimited and certainly unprecedented. The role of the plucky organisation being empowered by the Bill to bring a class action is, I am afraid, under some pressure. There is a gigantic inequality of legal arms.

The second reality on which the Government’s argument founders is the fact that data breaches, by their very nature, involve data being leaked about tens and tens of thousands of people. The idea that a small charity or a small representative body can round up positive authorisation from tens of thousands of people who have had their rights violated in order to then take Facebook, Google, Apple, Microsoft, Morrisons or Experian to court is laughable. I therefore ask the Government to reflect again on the unique asymmetry that such legal cases confront, and on the evidence of organisations such as Which?, which have had to try to bring cases such as that of Lloyd against Google. That evidence tells us loud and clear that a regime that requires opt-in will simply not work in practice. Our amendment would switch the emphasis. It would allow representative bodies to bring cases, allow people to opt out of cases and allow a collective opt-out.

The reason why the regime that we propose is much better than the one that Ministers proposed is to do with the protection of children’s data rights, which we do not think are properly taken care of. There is a fantasist that we imagine that groups of children will take Facebook to court because it might have leaked their data somewhere. We will therefore rely on
representative organisations to bring class actions on behalf of children. How on earth will Which? round up thousands of the nation’s children to secure their positive rights? Is it possible to bring such actions, which it is in the national interest to bring? That would be completely impossible. The measures that the Government propose are not only weak for adults but completely ineffective for children.

The Government’s proposals will allow for a reversal of the regime once we have taken into account the way the world works. Let us think about what that involves, though: allowing the system to fail before getting round to fixing it. The idea is that we introduce a regime knowing that it will not work, and watch the wholesale abuse and breach of people’s data rights. We then reflect on the reality that it is impossible for those people to secure justice under the regime that the Government have proposed. Then we decide that we will have a review, which will take a few months. Then Ministers will have to take a decision, and they will probably bring some proposals back to the House. At some point in the 2020s—perhaps the late 2020s—we may get round to having an effective regime to protect people’s data rights.

This is one of the defining questions on the Bill—the Government’s attitude to the amendments will define whether they are taking the defence of data rights seriously. We now know enough, from cases such as Lloyd against Google, about what works and does not work. The way the Which? trustees had to reflect on class actions brought against companies such as Google tells us enough about how the regime needs to operate.

If the Government are serious about taking on the double asymmetry—the asymmetry between the humble individual and the gigantic tech giants, and that between a single case and thousands of people having their data breached—they will accept the amendments. They were drawn up and tested very carefully. We sought expert legal counsel to get them right. We are grateful to the House for the fact that they have been framed nicely. I urge Ministers not to fail this basic test of judgment as to whether they are serious about protecting our data rights, and to accept the amendments.

Brendan O’Hara (Argyll and Bute) (SNP): It is a pleasure to serve under your chairmanship this afternoon, Mr Streeter.

I support amendment 154. We strongly recommend that if the Government are, as they claim to be, serious about providing the best possible data protection regime to achieve the gold standard that they often talk about providing the best possible data protection regime that if the Government are, as they claim to be, serious about protecting the rights of a data subject, when it considered that the rights of a data subject under the GDPR have been breached.

The right hon. Member for Birmingham, Hodge Hill, rightly said that the amendments would allow representative bodies to bring such cases, but would also allow individuals to opt out. Currently there is not a level playing field. If the Bill is not amended, the already uneven playing field will become impossibly uneven for individuals whose rights are breached or infringed—probably by a tech giant.

Collective redress was one of the most controversial and hotly debated issues when the Bill was in the House of Lords. The Government resisted all attempts to change it there. There have been slight amendments since then, and an understanding has been reached, but I feel that what the Government propose does not go nearly far enough to address the concerns expressed by Scottish National party and Labour Members.

Anna Fielder, a former chair of Privacy International, wrote: “Weak enforcement provisions were one of the widely acknowledged reasons why the current data protection laws, in the UK and elsewhere in Europe, were no longer fit for purpose in the big data age. As a result, it has been more convenient for organisations collecting and processing personal information to break the law and pay up if found out, than to observe the law—as profits made from people’s personal information vastly outweighed even the most punitive of fines.”

That is the situation we are in, and it is incumbent on legislators to level the playing field—not to make it even more uneven. However, as the Bill currently stands, it only enables individuals to request that such suitably qualified non-profit organisations take up cases on their behalf, rather than allowing the organisations themselves to highlight where they believe a breach of data protection law has occurred.

All too often, as has been pointed out on numerous occasions, individuals are the last people to know that their data has been unlawfully and in many cases illegally used. They depend on suitably qualified non-profit organisations, which are there to conduct independent research and investigations, to inform them that that is the case. Indeed, there was a very striking example recently in Germany, where the consumer federation took one of the tech giants to court over a number of platform breaches of current German data protection law, and it won. However, there are numerous examples across the world of organisations and groups highlighting bad or illegal practices that would hitherto probably have gone unnoticed here.

Privacy International recently published a report on the use and possible abuse of personal data connected to the rental car market. Which? has carried out research on online toys that are widely available in this country, which could pose serious child safety risks. The Norwegian consumer council has done similar work on toys, as well as exposing unlawful practices by health and dating apps.

Across the world, there are groups that do collective redress work very successfully in Belgium, Italy, Portugal, Spain, Sweden, Canada and Australia. I urge the Government to reconsider the matter and to see the great consumer benefits and protections that would come from accepting amendment 154. It would give not-for-profit organisations the right to launch complaints with a supervisory authority, as well as seeking judicial remedy, when it considered that the rights of a data subject under the GDPR had been breached.

I repeat that at the moment we have an uneven playing field. If the Bill goes through unamended it will become an impossible playing field for consumers, so I urge the Government to accept the amendment.

Darren Jones: I promise not to speak at every opportunity today, Mr Streeter; I am conscious that it is a Thursday and that Members have constituencies to get to, but on this point I will just add my support to the amendment tabled by my right hon. Friend the Member for Birmingham, Hodge Hill.
The Bill puts us in a position that we should not have been in in the first place. The Government’s original view was that they were not going to implement article 80 of the GDPR: they have now gone one step in that direction, and I support the aim that we go the whole hog.

I recognise from my work previous to being an MP that a lot of tech companies are not evil; they want to do the right thing and go about being successful as businesses. It was partly my job in the past to look at these areas of law on behalf of companies, and to work with campaigning groups, regulators and others. It was about being an internal voice to make sure that there was the correct balance within businesses was correct between considering consumers and being pro-business. This amendment would help to facilitate that conversation, because if bodies such as Which? that are private enforcers on behalf of consumers had these legal rights, then of course there would be an obligation on businesses to have ongoing dialogue and relationships. They would have to make sure that consumers’ concerns were at the forefront and that they were doing things in the right way.

The balance to be struck is really important. The Information Commissioner’s Office, for example, has lost quite a lot of staff to other companies recently. The Minister’s Department had to increase the salary bands for ICO staff to try to keep them there. In other sectors of the regulated economy, having private enforcers on behalf of consumers as a collective group works perfectly well for existing regulators.

In the telecommunications sector, in which I have worked in the past, there is Ofcom, which regulates the telecom sector, but there is also Which?, working as a private enforcer under the Consumer Rights Act 2015, which can act on behalf of consumers as a group. That works perfectly well and as my right hon. Friend said, private enforcers will not just start bringing these super-complaints every week, because the risk would be too high. They will only bring these super-complaints when they have failed in their dialogue and have no choice.

12.15 pm

Under the Consumer Rights Act 2015, where this mechanism exists today, we do not have endless vexatious super-complaints. There are actually some very effective super-complaints that work well in the interests of consumers, however. Some of the data breaches have involved groups as big as tens of millions of people.

I know from my own experience in other parts of law that we cannot always identify the individual involved. Sometimes they have moved on, or their contact details have changed, and we physically cannot get compensation to them. Under the Consumer Rights Act, again with the mechanism that came from European law—it is, a principle that has been copied across from the GDPR—compensation can be given to others on behalf of consumers as a group. It is given to consumer charities or consumer regulators to help facilitate their work. We ought to be alive to that possibility in data protection law.

That mechanism is normal and widely used at European Union law level to balance power between consumers and businesses. We have adopted it into UK law, as the
theme of the Bill and the GDPR as a whole, which is to empower individuals to take control of their own data. As yet we have no evidence that that is necessary.

**Liam Byrne:*** Let us take Uber—one of the most recent of the 200 data breaches listed on Wikipedia. In that case, 57 million records were leaked. How is one of those drivers going to take Uber to court to ensure justice?

**Margot James:** The GDPR places robust obligations on the data controller to notify all data subjects if there has been a breach that is likely to result in a high risk to their rights. That example is almost unprecedented and quite different—

**Liam Byrne:** It is not unprecedented. Look at the Wikipedia page on data breaches. There are 200 of them, including Uber, Equifax, AOL, Apple, Ashley Madison, Betfair—the list goes on and on. I want an answer to a very simple question. How is a humble Uber driver, who is busting a gut to make a living, going to find the wherewithal to hire a solicitor and take Uber to court? What is the specific answer to that question?

**Margot James:** If a data subject is sufficiently outraged, there is nothing to stop them contacting a group such as Which?, and opting into a group action. Furthermore, a range of enforcement options are open to the ICO. It can issue enforcement notices to compel the controller to stop doing something that is in breach of people’s data rights. As I said, there is nothing to stop a data subject opting into a group action.

**Liam Byrne:** There is only one major precedent for the kind of scenario the Minister has sketched out today, which is Various Claimants v. Wm Morrisons Supermarket plc—a case she knows well. That case illustrates the difficulties of opt-in. It is by far the largest group of data protection claimants ever put together. Even then, the total number of people who could be assembled was 5,000 out of 100,000 people whose data rights were breached. That was incredibly difficult and took a huge amount of time. Even if the claim succeeds, the 95% of people not covered by the claim will not receive justice. I am not quite sure what new evidence the Minister is waiting for so that she has enough evidence to activate the kind of proposals we are talking about today.

**Margot James:** As I said, the GDPR represents significant change. We believe we should test the effectiveness of the new enforcement scheme before we make further changes of the kind the right hon. Gentleman is suggesting. The Morrisons case was effective. The collective redress mechanism—group litigation orders—was used and was effective. The Information Commission will have new powers under the Bill to force companies to take action when there has been a breach of data.

There are other problems with amendment 154. First, like the right hon. Member for Birmingham, Hodge Hill, we are concerned about children’s rights. We would be concerned if a child’s fundamental data rights were weighed up and stripped away by a court without parents or legal guardians having had the opportunity to make the decision to seek redress themselves or seek the help of a preferred non-profit organisation. Once that judgment has been finalised, there will be no recourse for the child or the parent. They will become mere observers, which is unacceptable and makes a travesty of the rights they are entitled to enforce on their own account.

Secondly, we must remember that the non-profit organisations referred to in the amendment are, by definition, active in the field of data subjects’ rights. Although many will no doubt have data subjects’ interests at heart, some may have a professional interest in achieving a different outcome—for example, chasing headlines to promote their own organisation. That is why it is essential that data subjects are capable of choosing the organisation that is right for them or deciding not to partake in a claim that an organisation has advertised. The amendment would also allow an individual to bring a collective claim on behalf of other data subjects without their consent.

**Brendan O’Hara:** Does the Minister not accept, as I said earlier, that individuals are often the last people to know that their data has been breached and their rights have been infringed? For collective rights in hugely complicated areas, there must be a presumption that those rights are protected, and the Bill does not do that. I do not believe it reflects the principle that individuals are often the last people to know, and that they are the ones who need protecting.

**Margot James:** The Information Commissioner has powers to force companies to notify data subjects of any breach of data, and there is a legal requirement on companies so to do.

The amendment would allow an individual to bring a collective claim on behalf of other data subjects without their consent. We oppose it because it does not give people the protection of knowing that the entity controlling their claim is a non-profit organisation with a noble purpose in mind. I am pleased to say that, as I outlined this morning, the Government’s position was supported in the other place by the Opposition Front Benchers and the noble Baroness Kidron.

**Liam Byrne:** I am incredibly disappointed with the Minister’s response, and I am not quite sure I believe that she believes what she has been reading out. I hope that between now and Report, or whenever the amendment is pressed to a vote, she will have the opportunity to consult Which? and her officials. The reality is that for complex public policy decisions, whether relating to organ donation or auto-enrolment pensions, we have well-established procedures for opting out, rather than opting in. There has been strong cross-party support for that over the past seven or eight years, and it reflects a reality in new economic thinking. Behavioural economics shows that opt-out is often better than opt-in.

If the Government pursue that line of argument on Report, in the other place and through to Royal Assent, we will not permit the Minister ever again to refer to the Bill as a gold standard in data protection. It is a shoddy, tarnished bronze. She has sought to ensure that the legal playing field is tilted in the favour of large organisations and tech giants, and away from consumers and children. That will lead to a pretty poor state of affairs. We now have enough precedents to know that the regime she is
proposing will not work. This is not a theoretical issue; it has already been tested in the courts. Her proposal will not fix the asymmetry that potentially leaves millions of people without justice.

The idea that the Minister can present the Mororrison case as some kind of success when 95% of the people whose data rights were breached did not receive justice because they did not opt in to the class action betrays it all. She is proposing a system of redress that is good for the few and bad for the many. If that is her politics, so be it, but she will not be able to present the Bill as the gold standard if she persists with that argument.

The Chair: As I said, we will deal with the Opposition amendments later in our proceedings.

Amendment 115 agreed to.

Schedule 6, as amended, agreed to.

Clauses 23 and 24 ordered to stand part of the Bill.

Clause 25

MANUAL UNSTRUCTURED DATA USED IN LONGSTANDING HISTORICAL RESEARCH

Amendment made: 17, in clause 25, page 15, line 40, leave out “individual” and insert “data subject”.—(Margot James.)

Clause 25 makes provision about the processing of manual unstructured data used in longstanding historical research. This amendment aligns Clause 25(1)(b)(i) with similar provision in Clause 19(2).

Clause 25, as amended, ordered to stand part of the Bill.

Clause 26

NATIONAL SECURITY AND DEFENCE EXEMPTION

Question proposed, that the clause stand part of the Bill.

12.30 pm

Louise Haigh (Sheffield, Heeley) (Lab): It is a pleasure to serve under your chairmanship once again, Mr Streeter. I think it was about 18 months ago that we were in this very room, debating the Bill that became the Digital Economy Act 2017. We discussed at length the trade-off between the rights of data subjects, privacy, transparency and the need for Government access to data. In that context we were debating the rights of viewers of online pornography, rather than matters of national security. I note that the Government have had to delay the introduction of the regulations, because they failed to get to grips with the issues that we raised in Committee. I do not envy the new Minister, or, indeed, my right hon. Friend the shadow Minister, their task of attempting to get things right. It was one of the low points of my political career when I had to negotiate with the present Secretary of State for Digital, Culture, Media and Sport on what sexual acts would be blocked. I wish them both luck in taking the matter forward, and am glad I am dealing only with national security issues in the Bill that we are considering today.

As we come to crucial clauses that give Ministers and the security services a great deal more latitude, it is important for the Opposition to lay out key principles on national security certificates. Of course we support the legitimate interests of the intelligence services, as dictated by their statutory functions, including the safeguarding of national security. Of course we recognise that protecting citizens from harm often means striking a difficult balance between operational requirements and the rights of individuals who may fall within the scope of the investigations. We know that the security services take that seriously.

It is the Opposition’s duty, however, to scrutinise the Government’s approach, to ensure that any powers that explicitly allow the setting aside of citizens’ data rights under the Bill are proportionate and necessary, and that they will be overseen through appropriate safeguards. Clauses 26 and 27 provide for a national security certification regime allowing restriction of and exemption from a wide range of rights under the GDPR and the Bill on the basis of national security, and for defence purposes.

The Government state that national security falls outside the scope of EU law and, therefore, the GDPR, and that therefore any processing of personal data relating to national security will be governed by the applied GDPR. Article 4(2) of the treaty on the European Union provides that national security remains the sole responsibility of each member state. Despite that, EU data protection legislation provides for derogations for national security. If national security were entirely outside the scope of the EU treaty, such derogations would be unnecessary, so, as the Joint Committee on Human Rights argued, the provisions imply the retention of some level of EU scrutiny over derogations from EU data protection rights on the grounds of national security. It is thus not at all clear that the Government’s assertions about blanket national security exemptions are correct.

Furthermore, there is no clear definition of which entities will be covered by the extremely broad exemptions under subsection 1, which refers to “national security” and “defence purposes”. I am concerned that a measure allowing broad exemptions to the rights of citizens does not stipulate which entities will be entitled to jettison those rights. As was debated at length in the other place, there are no clear definitions of national security, or of the extended exemption for defence purposes, which goes beyond the Data Protection Act 1998, in the Bill or the explanatory notes. As the right hon. and learned Member for Rushcliffe (Mr Clarke) remarked during the passage of the Investigatory Powers Act 2016, “National security can easily be conflated with the policy of the Government of the day.”—[Official Report, 15 March 2016; Vol. 607, c. 850.]

As the Joint Committee on Human Rights concluded, “it is unclear why the authorities require such a breadth of exemptions from their obligations under the data protection regime.”

Before we move on to discuss our amendments to clause 26, I should be grateful if the Minister could assure us about the definitions of “national security” and “defence purposes” and in particular which entities they apply to.

The Chair: I think the amendments are to clause 27 of the Bill.

Brendan O’Hara: I rise to speak to amendment 161 and amendments 162 to 169.
The Chair: That is the next clause.

Brendan O’Hara: My apologies.

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): It is a pleasure to serve under your chairmanship, Mr Streeter. Clause 26 creates an exemption for certain provisions in the Bill only if that exemption is required for the purpose of safeguarding national security or for defence purposes. Where processing does not meet these tests, the exemption cannot apply. It is possible to exempt from most but not all the data protection principles the rights of data subjects, certain obligations on data controllers and processors, and various enforcement provisions, where required to safeguard national security or for defence purposes. In relation to national security, the exemption mirrors the existing national security exemption provided for in section 28 of the 1998 Act. The statutory framework has long recognised that the proportionate exemptions from the data protection principles and the rights of data subjects are necessary to protect national security. The Bill does not alter that position.

The exemption for defence purposes is intended to ensure the continued protection, security and capability of our armed forces and of the civilian staff who support them—not just their combat effectiveness, to use the outdated language of the 1998 Act. In drafting this legislation, we concluded that this existing exemption was too narrow and no longer adequately captured the wide range of vital activities that are undertaken by the Ministry of Defence and its partners. We have seen that all too obviously in the last two weeks.

Liam Byrne: On that point, will the Minister give way?

Victoria Atkins: If the right hon. Gentleman is going to disagree with me that combat effectiveness would be a very narrow term to describe the events in Salisbury, of course I will give way.

Liam Byrne: I actually wanted to ask about interpreters who support our armed forces. There is cross-party consensus that sometimes it is important to ensure that we grant leave to remain in this country to those very brave civilians who have supported our armed forces abroad as interpreters. Sometimes, those claims have been contested by the Ministry of Defence. Is the Minister confident and satisfied that the Ministry of Defence would not be able to rely on this exemption to keep information back from civilian staff employed as interpreters in support of our armed forces abroad when they seek leave to remain in this country?

Victoria Atkins: I cannot possibly be drawn on individual applications for asylum. It would be wholly improper for me to make a sweeping generalisation on cases that are taken on a case-by-case basis. I refer back to the narrow definition that was in the 1998 Act and suggest that our enlarging the narrow definition of combat effectiveness would mean including the civilian staff who support our brave troops.

The term “defence purposes” is intended to be limited in both application and scope, and will not encompass all processing activities conducted by the Ministry of Defence. Only where a specific right or obligation is found to be incompatible with a specific processing activity being undertaken for defence purposes can that right or obligation be set aside. The Ministry of Defence will continue to process personal information relating to both military and civilian personnel in a secure and appropriate way, employing relevant safeguards and security in accordance with the principles of the applied GDPR. It is anticipated that standard human resources processing functions such as the recording of leave and the management of pay and pension information will not be covered by the exemption.

Liam Byrne: I am sorry to press the Minister on this point, and she may want to write to me as a follow-up, but I think Members on both sides of the House have a genuine interest in ensuring that interpreters who have supported our troops abroad are able to access important information, such as the terms of their service and the record of their employment, when making legitimate applications for leave to remain in this country—not asylum—or sometimes discretionary leave.

Victoria Atkins: I am very happy to write to the right hon. Gentleman about that. The exemption does not cover all processing of personal data by the Ministry of Defence, but I am happy to write to him on that subject.

It may assist the Committee if I give a few examples of processing activities that might be considered to fall into the definition of defence purposes requiring the protection of the exemption. Such processing could include the collation of personal data to assist in assessing the capability and effectiveness of armed forces personnel, including the performance of troops; the collection and storage of information, including biometric data necessary to maintain the security of defence sites, supplies and services; and the sharing of data with coalition partners to support them in maintaining their security capability and the effectiveness of their armed forces. That is not an exhaustive list. The application of the exemption should be considered only in specific cases where the fulfilment of a specific data protection right or obligation is found to put at risk the security capability or effectiveness of UK defence activities.

The hon. Member for Sheffield, Heeley asked for a definition of national security. It has been the policy of successive Governments not to define national security in statute. Threats to national security are constantly evolving and difficult to predict, and it is vital that legislation does not constrain the security and intelligence agencies’ ability to protect the UK from new and emerging threats. For example, only a few years ago it would have been very difficult to predict the nature or scale of the threat to our national security from cyber-attacks.

Clause 26 does not provide for a blanket exemption. It can be applied only when it is required to safeguard national security or for defence purposes.

Daniel Zeichner: What weight does the Minister give to the written evidence that the Committee received from the Information Commissioner’s Office? It is obvious expert on this issue, and it addresses some of the points she made. It concludes that there is no threshold for when “defence purposes” are to be used, and that there is no guidance “for when it is appropriate to rely on the exemption.”
[Daniel Zeichner]

What weight does the Minister give to that, and what is her response to the concern raised by the Information Commissioner’s Office?

Victoria Atkins: Again, surely it is for the Executive—elected officials—to take responsibility for decisions that are made by data controllers in the Ministry of Defence. Obviously, the Department has considered the Information Commissioner’s representations, but this is not a blanket exemption. The high threshold can be met only in very specific circumstances.

Question put and agreed to.

Clause 26 accordingly ordered to stand part of the Bill.

Clause 27

National security: certificate

Louise Haigh: I beg to move amendment 161, in clause 27, page 17, line 2, leave out subsection (1) and insert—

“A Minister of the Crown must apply to a Judicial Commissioner for a certificate, if exemptions are sought from specified provisions in relation to any personal data for the purpose of safeguarding national security.”

This amendment would introduce a procedure for a Minister of the Crown to apply to a Judicial Commissioner for a National Security Certificate.

The Chair: With this it will be convenient to discuss the following:

Amendment 162, in clause 27, page 17, line 5, at end insert—

“(1A) The decision to issue the certificate must be—

(a) approved by a Judicial Commissioner,

(b) laid before Parliament,

(c) published and publicly accessible on the Information Commissioner’s Office website.

(1B) In deciding whether to approve an application under subsection (1), a Judicial Commissioner must review the Minister’s conclusions as to the following matters—

(a) whether the certificate is necessary on relevant grounds,

(b) whether the conduct that would be authorised by the certificate is proportionate to what it sought to be achieved by that conduct, and

(c) whether it is necessary and proportionate to exempt all provisions specified in the certificate.”

This amendment would ensure that oversight and safeguarding in the application for a National Security Certificate are effective, requiring sufficient detail in the application process.

Amendment 163, in clause 27, page 17, leave out lines 6 to 8 and insert—

“(2) An application for a certificate under subsection (1)—

(a) must identify the personal data to which it applies by means of a detailed description, and

This amendment would require a National Security Certificate to identify the personal data to which the Certificate applies by means of a detailed description.

Amendment 164, in clause 27, page 17, line 9, leave out subsection (2)(b).

This amendment would ensure that a National Security Certificate cannot be expressed to have prospective effect.

Amendment 165, in clause 27, page 17, line 9, at end insert—

“(c) must specify each provision of this Act which it seeks to exempt, and

(d) must provide a justification for both (a) and (b).”

This amendment would ensure effective oversight of exemptions of this Act from the application for a National Security Certificate.

Amendment 166, in clause 27, page 17, line 10, leave out “directly” and insert

“who believes they are directly or indirectly”

This amendment would broaden the application of subsection (3) so that any person who believes they are directly affected by a National Security Certificate may appeal to the Tribunal against the Certificate.

Amendment 167, in clause 27, page 17, line 12, leave out “, applying the principles applied by a court on an application for judicial review.”

This amendment removes the application to the appeal against a National Security Certificate of the principles applied by a court on an application for judicial review.

Amendment 168, in clause 27, page 17, line 13, leave out “the Minister did not have reasonable grounds for issuing” and insert

“it was not necessary or proportionate to issue”.

These amendments would reflect that the Minister would not be the only authority involved in the process of applying for a National Security Certificate.

Amendment 169, in clause 27, page 17, line 16, at end insert—

“(4A) Where a Judicial Commissioner refuses to approve a Minister’s application for a certificate under this Chapter, the Judicial Commissioner must give the Minister of the Crown reasons in writing for the refusal.

(4B) Where a Judicial Commissioner refuses to approve a Minister’s application for a certificate under this Chapter, the Minister may apply to the Information Commissioner for a review of the decision.

(4C) It is not permissible for exemptions to be specified in relation to—

(a) Chapter II of the applied GDPR (principles)—

(i) GDPR Article 24 – 32 inclusive,

(ii) GDPR Articles 35 – 43 inclusive,

(iii) Article 9 (processing of special categories of personal data),

(b) Chapter IV of the applied GDPR—

(i) GDPR Articles 24 – 32 inclusive,

(ii) GDPR Articles 35 – 43 inclusive,

(c) Chapter VIII of the applied GDPR (remedies, liabilities and penalties)—

(i) GDPR Articles 63 – 72 inclusive,

(ii) GDPR Article 84 (generally conditions for imposing administrative fines),

(iii) GDPR Article 84 (generally conditions for imposing administrative fines),

(d) Part 5 of this Act, or

(e) Part 7 of this Act.”

This amendment would require a Judicial Commissioner to intimate in writing to the Minister reasons for refusing the Minister’s application for a National Security Certificate and allows the Minister to apply for a review by the Information Commissioner of such a refusal.

Louise Haigh: With our amendments we seek to provide some oversight of and protections against the very broad definitions in this part of the Bill. I am afraid we are not content with the Minister’s assertions in her response on the previous clause.
As they currently stand, national security certificates give Ministers broad powers to remove individuals' rights with absolutely no oversight. If this is a matter for the Executive, as the Minister has just said, they must be subject to oversight and accountability when making such decisions, and as it stands there is absolutely none at all. The rights at risk from the exemption are the right to be informed when personal data is collected from individuals, which is in article 13 of the GDPR; the right to find out whether personal data against them is being processed, in article 15; and the right to object to automated decision making, in articles 21 and 22. Furthermore, the Information Commissioner's inspection, authorisation and advisory powers are set aside, which is why she and her office raised concerns, as my hon. Friend the Member for Cambridge set out.

It is not difficult to envisage examples of why those exemptions may be necessary. The Minister has laid some of them out; for instance, during the course of an ongoing national security investigation, the right of an individual to be informed that their data is being processed would not be appropriate. With these exemptions, there will inevitably be a need for appropriate safeguards to protect the rights of citizens. We are not yet convinced that the Bill contains them. That is what these amendments seek to tackle.

12.45 pm

As we have set out, any powers exercised in the interests of national security and defence must be necessary, proportionate and overseen by appropriate safeguards. Amendments 161 to 169 create a framework around which these necessary and proportionate powers can be used appropriately by Ministers and the security services. The current framework laid out in the Bill is extraordinarily narrow; yes, there will be a tribunal to determine the rights of the citizen, but the provisions of the Bill allow for that to happen only after the rights themselves have been infringed; they allow Ministers to detail the reasons for the certificate in only the vaguest possible terms; and they give the individual the power to appeal against the decision only within the narrow confines of a judicial review.

Amendment 161 would introduce a framework to give citizens judicial protection in the initial instance and greater rights. The provisions of clause 26(1) allow individuals to press for their rights only after the fact. The amendments would mirror the provisions of the Investigatory Powers Act 2016, which gives the Investigatory Powers Commissioner's office independent judicial oversight of public authorities' use of investigatory powers. Crucially, that office will consider whether it agrees with Ministers' decisions to authorise intrusive investigatory powers before they can come into effect. Judicial commissioners act independently of Government and can be removed from office only by resolution of each House, and in limited circumstances by the Prime Minister, for example through bankruptcy, disqualification as a company director, or conviction of an offence that carries a sentence of imprisonment.

If, under the 2016 Act, the exercise of a range of investigatory powers by public authorities—including the interception of communications, the acquisition and retention of communications data, equipment interference, intrusive surveillance, property interference, directed surveillance, covert human intelligence sources and bulk personal data sets—can be monitored prior to any potential breach of rights, it is not clear why a similar safeguard cannot take its place in the more limited provisions of this Bill.

Crucially, amendment 162 stipulates that the judicial commissioners should be entitled to make an assessment for a national security certificate based on the tests outlined today; namely, whether it is necessary and proportionate to issue a certificate. They should assess whether the certificate is necessary on relevant grounds, whether conduct authorised by the certificate would be proportionate, and whether it is necessary and proportionate to exempt all the provisions in question. The Government believe that the provisions in the Bill do not give controllers carte blanche to set aside rights and obligations, and that rights and obligations will be considered on a case-by-case basis, but they allow for obligations to be set aside with no oversight.

Citizens must have confidence that in the exercise of their duties, Ministers and the intelligence services are questioned to ensure that they are making the right decisions based on evidence. Amendments 163 and 165 would require the national security certificate to identify the personal data to which the certificate applies, and would require a Minister to provide a justification of why they are seeking an exemption under the Bill. It is not a big ask to require a Minister to state what data they are processing and for what purposes.

The Bill as it stands gives Ministers huge powers to set aside data rights, with no justification and providing only the bare minimum of information. A general description of the data in question would not alone be enough for the tribunal or the judicial commissioners to make a determination on whether the certificate was justified. Amendment 167 would allow the tribunal to consider the facts of the case, and it should be considered with the other amendments that I have spoken to. Judicial review, taken together with the limited information that the Government want to detail in the certificate, would leave only a very narrow angle open for a data subject whose rights had been unlawfully breached in a way that was neither necessary nor proportionate. That would allow the tribunal to consider the true facts of the case.

Finally, amendment 169 recognises the need for Ministers to be able to appeal the decision of the judicial commissioners in the event that they reject the application for a certificate. That appeal would go to the Information Commissioner and would stipulate that the judicial commissioner must set out the reasons why such an application was rejected.

As we have stated, we recognise how vital it is, operationally, for intelligence services and law enforcement to carry out their duties in the interest of national security, and no provision should get in the way of keeping our citizens from harm. The rights of data subjects must be protected, however, and where there are issues of national security, we have to get that balance right. We are seeking to help the Government do that by bringing the Bill into line with the safeguards that were added to the Investigatory Powers Act, to ensure necessity and proportionality without hindering operational requirement.

For an interference with rights to be in accordance with law, it must include safeguards against arbitrary interference. We contest that the provisions regarding
national security certificates fall short of that requirement. These clauses, unamended, would leave the Government wide open to legal challenge. We hope that the Minister will see the merit of our amendments and correct the Bill at this stage.

Brendan O’Hara: It may come as no surprise that I rise to speak in support of amendments 161 to 169. They are intended to challenge the Government’s plan to introduce a national security certification regime that will allow the restriction of and exemptions from a wide range of fundamental rights on the basis of national security and defence. Although it is absolutely right that, as a country, the UK has the ability to act in its own national security interest, I and many others are worried that the scale and scope of what is proposed in the Bill goes much further than the 1998 Act by widening the national security definition to include a further and, I would suggest, undefined range of defence purposes.

The Minister gave three or four examples earlier, but stressed that it was not an exhaustive list. Given the broad and indefinite nature of those national security exemptions, we are concerned that they do not meet the test of being both necessary and proportionate. How much confidence can we have that an individual’s fundamental rights will be best protected when the exemptions will be signed off by a Government Minister with little or no judicial oversight? It is also concerning that there appears to have been little or no attention to the harmful impact of exempting vast amounts of information from data protection safeguards by relying upon national security certificates.

As we heard earlier, the list of rights that are exempted, set out in clause 26, includes the right to be informed when data is being collected, the right to find out when personal data is being processed and the right to object to automated decision making. Those exemptions are to be exercised by a certificate, which, as I say, will be signed by a Minister, who will certify that an exemption from those rights and obligations is necessary for the purpose of safeguarding national security.

That means that, as the Bill is currently drafted, people’s rights could be removed by a politician without any form of judicial oversight. That cannot be right. We would argue most strongly that there has to be judicial oversight of any such decision, to prevent the removal of individual data protection rights from being permitted purely at the say-so of a Government Minister. I ask the Minister, how do the Government define national security and defence purposes in the context of the Bill? I certainly was not satisfied with the explanation we heard earlier on. I believe that these undefined terms are unnecessarily open-ended and broad, and open to vague interpretation. They could very well result in the removal of an individual’s rights unnecessarily. The lack of a clear definition of national security and defence purposes also means that people will be unable to foresee or understand when their rights will be overridden by the application of these exemptions. Surely that is incompatible with an individual citizen’s fundamental rights.

These exemptions, on the surface, are not limited to the UK’s intelligence and security services. As we heard when debating part 2 of the Bill, which deals with general processing, they broadly permit public authorities, and even private corporations on occasion, to invoke national security and defence as a reason to cast aside privacy rights. Can the Minister explain if, how, and under what circumstances a public authority or private company could invoke national security and defence as a reason to cast aside privacy rights?

That brings me to necessity and proportionality, which are fundamental principles when looking at exemptions from data protection, and which will be examined extremely closely by the European Commission and its legal team when it decides on the UK’s suitability for adequacy after Brexit. The principles of necessity and proportionality are enshrined in the European convention on human rights. A Minister must take them into account when they consider restricting or limiting an individual’s rights, such as those under article 8, the right to privacy.

As the Bill stands, no conditions or tests are imposed on a Minister’s decision to withdraw an individual’s personal data protection rights by issuing a national security certificate. There is no limitation on how a national security certificate should run or how long it should operate for. There is no obligation to review the ongoing necessity of having a live certificate. In effect, a certificate is open-ended and indefinite. My concern is that that may allow the state to use a certificate for activities for which it was not considered relevant or appropriate by the Minister when it was first issued or signed.

That loophole cannot be considered proportionate or necessary. The certificates have to be time-limited. That does not mean that once a certificate has expired it cannot be re-certified, but it would ensure that certificates that are no longer necessary or that have been used beyond their original remit do not continue indefinitely. Perhaps the Minister could explain why she thinks such a system could not work, and why it would not be in the best interest of the state and of protecting an individual’s rights.

As with everything we do, including everything we have done in this area in the past couple of years, the Bill has to be seen against the backdrop of Brexit. Not only do we have to comply with the GDPR, but we have to do so in a way that means the United Kingdom will achieve the vital, much sought after adequacy decision from the European Commission. We also have to keep our laws consistent with EU law to maintain that adequacy status. I fear that the widespread use of exemptions and, perhaps more worryingly, the undefined range of defence purposes could deal a severe blow to the UK achieving an adequacy decision from the European Commission.

Can the Minister tell me whether the Government have been given cast-iron guarantees that the new and undefined range of defence purposes will be consistent with EU law, to allow us not just to achieve adequacy but to maintain adequacy post Brexit?

The Chair: I will call the Minister to respond, but before she responds to that point, she wishes to correct the record in relation to a previous point, which I am happy to permit.

Victoria Atkins: On reflection, I would not wish the hon. Member for Cambridge to understand my earlier answer to mean that a Minister makes a decision on defence purposes. I apologise to him if that was not clear. It is
the data controller at the Ministry of Defence who makes that decision. The data controller is accountable to Ministers and in due course to domestic courts. I hope that clarifies that.

The Chair: And now the response to amendment 161.

Victoria Atkins: I think I am going to be cut off for lunch, Mr Streeter.

The Chair: It is up to the Committee what time we adjourn for lunch, of course, and the Minister may wish to speak quite rapidly.

The Lord Commissioner of Her Majesty’s Treasury (Nigel Adams): Much as I would like the Minister to speak rapidly, I will move the Adjournment.

Ordered, That the debate be now adjourned.—(Nigel Adams.)

12.59 pm

Adjourned till this day at Two o’clock.
CONTENTS

Clauses 27 to 30 agreed to, one with amendments.
Schedule 7 agreed to.
Clauses 31 to 35 agreed to.
Schedule 8 agreed to, with an amendment.
Clauses 36 to 86 agreed to, some with amendments.
Adjourned till Tuesday 20 March at twenty-five minutes past Nine o’clock.
Written evidence reported to the House.
No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Monday 19 March 2018
The Committee consisted of the following Members:

**Chairs:** †David Hanson, Mr Gary Streeter

† Adams, Nigel (Lord Commissioner of Her Majesty’s Treasury)
† Atkins, Victoria (Parliamentary Under-Secretary of State for the Home Department)
† Byrne, Liam (Birmingham, Hodge Hill) (Lab)
† Clark, Colin (Gordon) (Con)
† Elmore, Chris (Ogmore) (Lab)
† Haigh, Louise (Sheffield, Heeley) (Lab)
† Heaton-Jones, Peter (North Devon) (Con)
† Huddleston, Nigel (Mid Worcestershire) (Con)
† Jack, Mr Alister (Dumfries and Galloway) (Con)
† James, Margot (Minister of State, Department for Digital, Culture, Media and Sport)
† Jones, Darren (Bristol North West) (Lab)
† Lopez, Julia (Hornchurch and Upminster) (Con)
† McDonald, Stuart C. (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP)
Murray, Ian (Edinburgh South) (Lab)
† O’Hara, Brendan (Argyll and Bute) (SNP)
Snell, Gareth (Stoke-on-Trent Central) (Lab/Co-op)
† Warman, Matt (Boston and Skegness) (Con)
† Wood, Mike (Dudley South) (Con)
† Zeichner, Daniel (Cambridge) (Lab)

Kenneth Fox, Committee Clerk

† attended the Committee
Amendment proposed (this day): 161, in clause 27, page 17, line 2, leave out subsection (1) and insert—

“A Minister of the Crown must apply to a Judicial Commissioner for a certificate, if exemptions are sought from specified provisions in relation to any personal data for the purpose of safeguarding national security.”—(Louise Haigh.)

This amendment would introduce a procedure for a Minister of the Crown to apply to a Judicial Commissioner for a National Security Certificate.

Question again proposed, That the amendment be made.

The Chair: I remind the Committee that with this we are discussing the following:

Amendment 162, in clause 27, page 17, line 5, at end insert—

“(1A) The decision to issue the certificate must be—

(a) approved by a Judicial Commissioner,

(b) laid before Parliament,

(c) published and publicly accessible on the Information Commissioner’s Office website.

(1B) In deciding whether to approve an application under subsection (1), a Judicial Commissioner must review the Minister’s conclusions as to the following matters—

(a) whether the certificate is necessary on relevant grounds,

(b) whether the conduct that would be authorised by the certificate is proportionate to what it sought to be achieved by that conduct, and

(c) whether it is necessary and proportionate to exempt all provisions specified in the certificate.”.

This amendment would ensure that oversight and safeguarding in the application for a National Security Certificate are effective, requiring sufficient detail in the application process.

Amendment 163, in clause 27, page 17, leave out lines 6 to 8 and insert—

“(2) An application for a certificate under subsection (1)—

(a) must identify the personal data to which it applies by means of a detailed description, and”.

This amendment would require a National Security Certificate to identify the personal data to which the Certificate applies by means of a detailed description.

Amendment 164, in clause 27, page 17, line 9, leave out subsection (2)(b).

This amendment would ensure that a National Security Certificate cannot be expressed to have prospective effect.

Amendment 165, in clause 27, page 17, line 9, at end insert—

“(c) must specify each provision of this Act which it seeks to exempt, and

(d) must provide a justification for both (a) and (b).”.

This amendment would ensure effective oversight of exemptions of this Act from the application for a National Security Certificate.

Amendment 166, in clause 27, page 17, line 10, leave out “directly” and insert

“who believes they are directly or indirectly”. This amendment would broaden the application of subsection (3) so that any person who believes they are directly affected by a National Security Certificate may appeal to the Tribunal against the Certificate.

Amendment 167, in clause 27, page 17, line 12, leave out “, applying the principles applied by a court on an application for judicial review.”.

This amendment removes the application to the appeal against a National Security Certificate of the principles applied by a court on an application for judicial review.

Amendment 168, in clause 27, page 17, line 13, leave out “the Minister did not have reasonable grounds for issuing” and insert

“It was not necessary or proportionate to issue”.

These amendments would reflect that the Minister would not be the only authority involved in the process of applying for a National Security Certificate.

Amendment 169, in clause 27, page 17, line 16, at end insert—

“(4A) Where a Judicial Commissioner refuses to approve a Minister’s application for a certificate under this Chapter, the Judicial Commissioner must give the Minister of the Crown reasons in writing for the refusal.

(4B) Where a Judicial Commissioner refuses to approve a Minister’s application for a certificate under this Chapter, the Minister may apply to the Information Commissioner for a review of the decision.

(4C) It is not permissible for exemptions to be specified in relation to—

(a) Chapter II of the applied GDPR (principles)—

(i) GDPR Articles 24 – 32 inclusive,

(ii) GDPR Articles 35 – 43 inclusive,

(iii) Article 9 (processing of special categories of personal data),

(b) Chapter IV of the applied GDPR—

(i) GDPR Articles 24 – 32 inclusive,

(ii) GDPR Articles 35 – 43 inclusive,

(c) Chapter VIII of the applied GDPR (remedies, liabilities and penalties)—

(i) GDPR Article 83 (general conditions for imposing administrative fines),

(ii) GDPR Article 84 (penalties),

(d) Part 5 of this Act, or

(e) Part 7 of this Act.”.

This amendment would require a Judicial Commissioner to intimate in writing to the Minister reasons for refusing the Minister’s application for a National Security Certificate and allows the Minister to apply for a review by the Information Commissioner of such a refusal.

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): Thank you, Mr Hanson. It is a pleasure to serve under your chairmanship again.
I will first provide some context for this part of the Bill. The provisions in the Bill relating to national security exemptions and certificates are wholly in line with the provisions in the Data Protection Act 1998 and its predecessor, the Data Protection Act 1984. What we are doing in the Bill is preserving an arrangement that has been on the statute book for more than 30 years and has been operated by successive Governments.

The national security exemption is no different in principle from the other exemptions provided for in the Bill. If it is right that certain provisions of data protection legislation can be disapplied for reasons of, for example, crime prevention or taxation purposes, or in pursuit of various regulatory functions, without external approval, surely it is difficult to take issue with the need for an exemption on the grounds of national security on the same basis.

Louise Haigh (Sheffield, Heeley) (Lab): The Minister is absolutely right that the provisions mirror those in the DPA. That is exactly why we take issue with them. They mirror unacceptable preventions of rights in the tribunal appeal process, but do not mirror the rights in the Investigatory Powers Act 2016. Why were safeguards were put in place in that Act, but will not apply in this Bill?

Victoria Atkins: If I understand the hon. Lady’s argument correctly, she has presented the judicial commissioners as permitting, for example, warrant to be granted. Having sat through the Joint Committee on the Draft Investigatory Powers Bill and then the Public Bill Committee, I can tell her that I am afraid that is not how that Act works. What happens is that the Secretary of State grants the warrant and then that decision is overseen by the judicial commissioner. I will come on to the difference between the Investigatory Powers Act and this Bill in due course, because the terminology used draws on that in the Investigatory Powers Act, but that Act is very different from this Bill, which is about the processing of data, in its engagement with people and their rights.

Darren Jones (Bristol North West) (Lab): Will the Minister give way on that point?

Victoria Atkins: If I may, I will make some progress. Along with existing provisions in section 28 of the 1998 Act, clause 27 provides for a certificate signed by a Minister of the Crown certifying that exemption from specified data protection requirements is required for the purposes of safeguarding national security. There are equivalent provisions in parts 3 and 4 of the Bill. Such a certificate is conclusive evidence of that fact, for example in any legal proceedings. That is the point about the certificates—they only come into play if the exemption or restriction is actually applied.

The certificate provides evidence that the exemption or restriction is required for the purpose of safeguarding national security. It therefore has relevance only in the event that, first, the exemption or restriction is applied to the data in question and, secondly, there is a need to rely on the certificate as conclusive evidence in proceedings to establish that the exemption or restriction is required for the statutory purpose.

Louise Haigh: But what the national security certificate does not require is a statement of what data is being processed or the exemptions under which the Ministry of Defence or the intelligence services require it. That is what our amendments seek to introduce. If the Bill proceeds unamended, national security certificates would require only very broad details and no information on what data was being processed. It would therefore not be very likely that a tribunal would be able to oppose the decision on the basis of a judicial review.

Victoria Atkins: I have a copy of a live certificate granted by the then Secretary of State, David Blunkett, on 10 December 2001. In the certificate, he sets out in summary the reasons why the certificate has been granted, including:

“The work of the security and intelligence agencies of the Crown requires secrecy.”

I assume hon. Members do not disagree with that. Another reason is:

“The general principle of neither confirming nor denying whether the Security Service processes data about an individual, or whether others are processing personal data for, on behalf of with a view to assist or in relation to the functions of the Security Service, is an essential part of that secrecy.”

Again, I assume that hon. Members do not disagree with that. As I said, this is a live certificate that has been given to the Information Commissioner, and is in the public domain for people to see and to check should they so wish. Those reasons are given in that certificate.

Louise Haigh: That is wonderful, but the Bill does not require that. It is great that my noble Friend Lord Blunkett put that on his national security application, but the Bill does not require that in law, so I am afraid that it is not a sufficient argument against the amendments that we have tabled.

Victoria Atkins: What we are doing is transposing the requirements of the Data Protection Act 1998 into the Bill. It is difficult to see a situation in which a national security certificate will be granted on the basis that the work of the security and intelligence agencies of the Crown does not require secrecy.

Peter Heaton-Jones (North Devon) (Con): Is there not a bigger, more general overall point here, which is that we should not be considering doing anything in Committee that risks making it more difficult for the security services to protect us? This week of all weeks, surely that should be uppermost in our minds.

Victoria Atkins: Very much so—indeed, this debate ran through the passage of the Investigatory Powers Act 2016, which was one of the most scrutinised pieces of legislation. Senior parliamentarians who served on the Committee on that Act during long careers in this House, including the then Minister, my right hon. Friend the Member for South Holland and The Deepings (Mr Hayes), said that it was an incredibly well scrutinised Bill. There was constant debate about the battle, or tension, between ensuring the national security of our country in the most transparent way possible, and the fact that by definition there has to be some secrecy and confidentiality about the ways in which the security agencies work.
What was important in the debates on that Act, as it is in those on the current Bill, was making it clear that the idea that rogue civil servants or security agents can run around with people’s information with no checks is very wrong. We are replicating in the Bill the system that has been used for the past 30 years, because we consider that that system has the appropriate and necessary safeguards in the often very fast-moving context of national security situation.

Louise Haigh: Will the Minister give way?

Victoria Atkins: I will make a little progress, then I will take more interventions.

To be absolutely clear, a national security exemption is applied not by a Minister but by a data controller. Data controllers—be they the intelligence services, the Ministry of Defence or any other body—are well placed to make the determination, given that they will have a detailed understanding of the operational context and the extent to which departure from the requirement of the general data protection regulation—or parts 3 or 4 of the Bill as the case may be—is necessary to safeguard national security. In short, a data controller decides whether the national security exemption should be applied in a particular case, and the certificate is the evidence of the need for such an exemption in the event that someone challenges it.

Louise Haigh: Will the Minister give way?

Victoria Atkins: I will give an example first, because I think it is so important. I fear that a bit of misunderstanding has crept in. Let us take the example of a subject access request. Mr Smith asks an intelligence service whether it is processing personal data concerning him and, if so, for information about that data under clause 94. The intelligence service considers whether it is processing personal data, which it will have obtained under its other statutory powers, such as the Regulation of Investigatory Powers Act 2000 or the Investigatory Powers Act 2016.

If the agency determines that it is processing personal data relating to Mr Smith, it then considers whether it is able to disclose the data, or whether a relevant exemption is engaged. For the agency, the key consideration will be whether disclosing the data would damage national security, for example by disclosing sensitive capabilities or alerting Mr Smith to the fact that he is a subject of investigation. If disclosure does not undermine national security and no other exemption is relevant, the intelligence service must disclose the information. However, if national security would be undermined by disclosure, the agency will need to use the national security exemption in relation to processing any personal data relating to Mr Smith.

If the intelligence service does not process any personal data relating to Mr Smith, it will again have to consider whether disclosing that fact would undermine national security, for example by revealing a lack of capability, which could be exploited by subjects of investigation. That is why, on occasion, when such requests are made, a “neither confirm nor deny” response may be necessary, because either confirming or denying may in itself have ramifications, not only in relation to Mr Smith but in relation to other aspects of national security.

Mr Smith may complain to the Information Commissioner about the response to his request for information. The intelligence service may then be required to demonstrate to the commissioner that the processing of personal data complies with the requirements of part four of the Bill, as set out in clause 102, and that it has responded to the request for information appropriately.

If, in legal proceedings, Mr Smith sought to argue that the national security exemption had been improperly relied upon, a national security certificate could be used as conclusive evidence that the national security exemption was required to safeguard national security. Any person who believed they were directly affected by the certificate could of course appeal against it to the upper tribunal, as set out in clause 111.

Liam Byrne (Birmingham, Hodge Hill) (Lab): The Minister is setting out the mechanics of the system with admirable clarity. The point in dispute, though, is not the mechanics of the process but whether the data controller is able—unilaterally, unchecked and unfettered—to seek a national security exemption. Anyone who has worked with the intelligence agencies, either as a Minister or not, knows that they take parliamentary oversight and the defence of parliamentary supremacy extremely seriously.

What we are seeking with this amendment is to ensure that a data controller does not issue a national security certificate unchecked, and that instead there is an element of judicial oversight. The rule of law is important. It should be defended, protected and enhanced, especially when the data collection powers of the intelligence services are so much greater than they were 30 years ago when data protection legislation was first written.

Victoria Atkins: The Government fully accept that national security certificates should be capable of being subject to judicial oversight. Indeed, the current scheme—both under the 1998 Act and this Bill—provides for just that. However, the amendments would radically change the national security certificate regime, because they would replace the existing scheme with one that required a Minister of the Crown to apply to a judicial commissioner for a certificate if an exemption was sought for the purposes of safeguarding national security, and for a decision to issue a certificate to be approved by a judicial commissioner.

This, again, is the debate that we had when we were considering the Investigatory Powers Act 2016. There were some who would have preferred a judicial commissioner to make the decision about warrant application before the Secretary of State. However, Parliament decided that it was not comfortable with that, because it would have meant a great change. For a member of the judiciary to certify on national security issues, rather than a member of the Executive—namely the Prime Minister or a Secretary of State—would have great constitutional implications.

There were great debates about the issue and the House decided, in its wisdom, that it would maintain the constitutional tradition, which is that a member of the Executive has the ultimate responsibility for national
security, with, of course, judicial oversight by judicial commissioners and by the various tribunals that all these powers are subject to. The House decided that the decision itself must be a matter for a Minister of the Crown, because in the event—God forbid—that there is a national security incident, the House will rightly and properly demand answers from the Government of the day. With the greatest respect, a judicial commissioner cannot come to the Dispatch Box to explain how the Government and those assisting them in national security matters have responded to that situation. That is why we have this fine constitutional balance, and why we have adopted in the Bill the regime that has been in place for 30 years.

2.15 pm

We are keen to deal with the point about the Investigatory Powers Act and the obtaining of information. The nature of the conduct carried out in the case of an authorised warrant under the IPA is entirely different from the operation of the national security exemption and the use of national security certificates. Warrants authorise operational activity, which may have an impact on the right to respect for a private life when that is necessary and proportionate for a statutory purpose. They are about obtaining information, not processing it. In the context of the Bill, the application of an exemption would prevent an individual from ascertaining what personal data is being processed by a data controller.

The hon. Member for Sheffield, Heeley mentioned equipment interference, but there are other types of warranty in the Investigatory Powers Act, such as for interception of communications. That is about the obtaining of information—that can be quite intrusive, which is why Parliament has placed a number of judicial and other oversights on it—but this Bill is about the processing of personal data. It is quite a different thing.

In the impact on the data subject, the national security exemption is similar in kind to the other exemptions in the Bill, which have been approved in the other place and in this Committee’s debates thus far.

**Darren Jones:** Before the Minister does that, will she consider the regime that we have in place, because we simply do not have the right kind of judicial oversight of the information gathering powers that are now available to our intelligence services. Our intelligence services are very good, and they need to be allowed to do their job, but they will be allowed to do that job more effectively—and without additional risks to our adequacy—if there is some kind of judicial oversight in the right timeframe of the decisions that are taken.

**Liam Byrne:** I have spoken to the outgoing Council of Europe information commissioner about the issue, and he has put on the record his grave reservations about the regime that we have in place, because we simply do not have the right kind of judicial oversight of the information gathering powers that are now available to our intelligence services. Our intelligence services are very good, and they need to be allowed to do their job, but they will be allowed to do that job more effectively—and without additional risks to our adequacy—if there is some kind of judicial oversight in the right timeframe of the decisions that are taken.
Victoria Atkins: The obtaining of information is potentially intrusive and often extremely time-sensitive. For the processing of information, particularly in the case of a subject access request, once we have met the criteria for obtaining it, separate judicial oversight through the upper tribunal is set out in the Bill, as well as ministerial oversight. They are two separate regimes.

There is extra oversight in the 2016 Act because obtaining information can be so intrusive. The right hon. Gentleman will appreciate that I cannot go into the methodology—I am not sure I am security-cleared enough to know, to be honest—but obtaining information has the potential to be particularly intrusive, in a way that processing information gathered by security service officials may not be.

Liam Byrne: I reassure the Minister that I went through the methodologies during my time at the Home Office. The justification that she still needs to lay out for the Committee—she is perhaps struggling to do so—is why there should be one set of judicial oversight arrangements for obtaining information and another for processing it. Why are they not the same?

Victoria Atkins: There might be many reasons why we process information. The end result of processing might be for national security reasons or law enforcement reasons—my officials are scribbling away furiously, so I do not want to take away their glory when they provide me with the answer.

I have an answer on the Watson case, raised by the hon. Member for Sheffield, Heeley, which dealt with the retention of communications by communications service providers. Again, that is an entirely different scenario from the one we are talking about, where the material is held by the security services.

Amendment 161 goes further than the 2016 Act, because it places the decision to issue a certificate with the judicial commissioner. As I have said, national security certificates come into play only to serve in legal proceedings as conclusive evidence that an exemption from specified data protection requirements is necessary to protect national security—for example, to prevent disclosure of personal data to an individual under investigation, when such disclosure would damage national security. The certificate does not authorise the required processing. It is not something that can be used as conclusive evidence of the national security exemption by the intelligence services and others is both sufficiently foreseeable for the purposes of article 8 of the European convention on human rights, and accountable. The accountability is ensured by the power to challenge certificates when they are issued, and that is something that has real teeth. The accountability is strengthened by the provision in clause 130 for the publication of certificates. The documents we are discussing will therefore be in the public domain—indeed, many of them are already. But it will now be set out in statute that they should be in the public domain.

Amendments 166 to 168 relate to the appeals process. Amendment 166 would broaden the scope for appealing a national security certificate from a person “directly affected” by it to someone who “believes they are directly or indirectly affected” by it. I wonder whether the Opposition did any work on the scope of the provision when drafting it, because the words “indirectly affected” have the potential to cause an extraordinary number of claims. How on earth could that phrase be defined in a way that does not swamp the security services with applications from people who consider that they might be indirectly affected by a decision relating to a national security matter? I do not see how that can be considered practicable.

Louise Haigh: As I have already said, the issue is that the judicial review process for appeal is incredibly narrow and limited. Under section 28 of the DPA, where an individual requests to access his or her data that is subject to a certificate, they will merely be informed that they have been given all the information that is required under the Act. They would not be informed that their data is being withheld on the grounds of a national security certificate. That means that it is impossible for them to know whether they even have the right to appeal under a judicial review, and they do not have the information available to allow them take that judicial review case forward. That is why the amendment is drafted in this way. If the Minister would like, she can suggest some alternative wording that would solve the problem.

Victoria Atkins: We get to the nub of the problem. Is the hon. Lady seriously suggesting that the security services should notify someone who puts in an access request that they are the subject of an investigation? That is the tension facing the security services. That is why we have internationally met standards, with regard to article 108 of the convention, which the Bill complies with. That is why we have to build in all these safeguards, to try to ensure that those people who intend ill will to this country do not benefit from our natural wish to be as transparent as possible when dealing with people’s personal data.

Louise Haigh: I have already explained that there would of course be an exemption for not informing individuals if they were under surveillance or being processed, but there are not sufficient oversights, safeguards or appeals. In the absence of any of those three, the Minister has to accept that there are absolutely no checks and balances on the exemptions listed under the clause.

Victoria Atkins: There most certainly are: they have the right to appeal to the upper tribunal.

Louise Haigh: Under judicial review?
Victoria Atkins: Yes. The upper tribunal reviews the material and applies the judicial review test. Again, we had this debate in relation to the Investigatory Powers Act 2016, which Parliament passed, in relation to the test that applied in the later appeal stages, following the grant of a warrant. This Bill has been drafted to comply with the modernised convention 108 of the Council of Europe. This is why it is in this way. It reflects the past 30 years’ worth of practice but meets international standards as they exist at the moment, which I hope reassures the hon. Member for Bristol North West.

2.30 pm

If someone is the subject of investigation or suspicion, and the security services neither confirm nor deny, when someone who is not under suspicion puts in an application, the great tension for the security services is whether they answer differently in one case from another. In such circumstances that would have ramifications, because people will work out that this answer has been given or this answer has not been given. Of course there is a tension. That is why the exemptions exist and why so much emphasis is placed on the data controller, and that is why it meets the international standard as expected by the modernised Council of Europe convention.

Peter Heaton-Jones: On the specific narrow point, is it not the case that clause 130 already provides for the publication of certificates, so the amendment is simply not necessary? On the wider point—at the risk of repeating my earlier one—I fear that we are at risk of stumbling into a law of unintended consequences where we will make it more difficult for our security services to do the job that we want them to do. While we have been sitting here, I saw on my phone that the international community has recognised that what happened in Salisbury is the first recorded attack using a nerve agent on a European country since 1945. Let us remember that.

Victoria Atkins: That is a particularly sobering development. I know that we all feel the gravity of our responsibilities when considering the Bill in the context of national security today. I am grateful to my hon. Friend.

Matt Warman (Boston and Skegness) (Con): The Minister and I served on the Draft Investigatory Powers Bill Joint Committee and we had many debates on this subject. It struck me that the House was at its best when we passed the Investigatory Powers Bill on Third Reading, with the support of the Labour party, having had these debates. It is frustrating that today of all days, as my hon. Friend says, we should go over that ground again having already reached a useful consensus.

Victoria Atkins: On the judicial review point, the test was debated at length in the Joint Committee, in the Public Bill Committee and on the Floor of the House. The House passed that Act with cross-party consensus, as my hon. Friend has said, so I do not understand why we are having the same debate.

Liam Byrne: Anyone who has spent time working with our intelligence agencies knows that they see their mission as the defence of parliamentary democracy. They believe in scrutiny and oversight, which is what we are trying to insert in the Bill. The reason the Investigatory Powers Bill was passed in that way was because we were successful in ensuring that there were stronger safeguards. The Minister has been unable to explain today why the safeguarding regime should be different for the processing of data as opposed to the obtaining of data. We have heard no convincing arguments on that front today. All that we are seeking to do is protect the ability of the intelligence agencies to do their job by ensuring that a guard against the misuse of their much broader powers is subject to effective judicial oversight, and not in public but in a court.

Victoria Atkins: For the security services to have obtained data under the Investigatory Powers Act, they will have passed through the various safeguards that Parliament set out in that Act. Once that data is obtained, it follows that the permission that the judicial commissioner will have reviewed will still flow through to the processing of that information. Our concern here is certain requirements of the data protection regime. The decision to disseminate information under that regime must rest with the intelligence agencies, with oversight. The Bill provides for those decisions to be appealed. That is as it should be. It should not be for a judicial commissioner to take over the decision of the data controller, who is processing applications and information in real time, often in situations that require them to act quickly. Likewise, whether to grant a certificate, which will be in the public domain, must be a decision for a member of the Executive, not the judiciary.

I assume that no work has been done to measure the scope of amendment 166, but allowing the clause to cover people indirectly affected could have enormous consequences for the security services, which already face great pressures and responsibilities.

Amendments 167 and 168 would remove the application of judicial review principles by the upper tribunal when considering an appeal against a certificate. They would replace the “reasonable grounds for issuing” test with a requirement to consider whether issuing a certificate was necessary and proportionate. Again, that would be an unnecessary departure from the existing scheme, which applies the judicial review test and has worked very well for the past 30 years.

In applying judicial review principles, the upper tribunal can consider a range of issues, including necessity, proportionality and lawfulness. As we set out in our response to the report of the House of Lords Constitution Committee, that enables the upper tribunal to consider matters such as whether the decision to issue the certificate was reasonable, having regard to the impact on the rights of the data subject and the need to safeguard national security. The Bill makes it clear that the upper tribunal has the power to quash the certificate if it concludes that the decision to issue it was unreasonable.

I hope that I have answered the concerns of the right hon. Member for Birmingham, Hodge Hill about how certificates are granted and about the review process when a subject access request is made and the certificate is applied. We must recognise that the Bill does not weaken a data subject’s rights or the requirements that must be met if an exemption is to be relied on; it reflects the past 30 years of law. Perhaps I missed it, but I do not think that any hon. Member has argued that the Data Protection Act 1998 has significant failings.
Liam Byrne: As the Minister well knows, the debate internationally is a result of the radical transformation of intelligence agencies’ ability to collect and process data. There is an argument, which has been well recognised in the Council of Europe and elsewhere, that where powers are greater, oversight should be stronger.


Liam Byrne: It is about obtaining information, not processing it.

Victoria Atkins: The safeguards that apply once the information has been obtained—

Liam Byrne: There aren’t any safeguards!

The Chair: Order. I realise that the right hon. Gentleman feels strongly about the issue, but if he wishes to intervene, he must stand. If not, he must remain quiet and take it on the chin.

Victoria Atkins: The Government have listened to the concerns of the House of Lords. We added clause 130 in the Lords to provide for the publication of national security certificates by the Information Commissioner, so that they would be easily accessible to anyone who wished to mount a subject access request, and could be tested accordingly. In her briefing to noble Lords about the Bill, the Information Commissioner said that the clause was “very welcome as it should improve regulatory scrutiny and foster greater public trust and confidence in the use of national security certificate process.”

It will also ensure that any person who believes that they are directly affected by a certificate will be better placed to exercise their appeal rights.

The Bill’s approach to national security certificates is tried and tested. We rely on those 30 years of experience placed to exercise their appeal rights.

The safeguards and oversights are not built into the Bill in the way they were in the Investigatory Powers Act 2016. There is no clear argument why those safeguards should be in place for collection, but not for processing. The Minister has constantly relayed that that decision is based on 30 years’-worth of data but, as has already been said, the scope for the collection and processing of data is so far transformed, even from when the Data Protection Act was written in 1998, that the oversights and safeguards need to be transformed as well. That is why we are proposing these amendments.

The Joint Committee on Human Rights has suggested that the exemptions put forward in the Bill are not legal and introduce arbitrary interferences into people’s privacy rights. It is this Committee’s responsibility to ensure that the amendments pass. That is not trivialising the issue, but ensuring that there is a proper debate about security and the individual’s data subject rights. That is why we will press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 10.

Division No. 7]

AYES

Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren

NOES

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

Question accordingly negatived.

Clause 27 ordered to stand part of the Bill.

The Chair: Members will note that there are a number of clauses on the selection list to which no amendments have been tabled. I propose to start grouping such clauses together in order to speed progress. However, Members still have the right to tell me that they wish to speak to, or vote on, an individual clause.

Clauses 28 and 29 ordered to stand part of the Bill.

Clause 30

MEANING OF “COMPETENT AUTHORITY”

Amendments made: 18, in clause 30, page 19, line 4, after “specified” insert “or described”.

This amendment changes a reference to persons specified in Schedule 7 into a reference to persons specified or described there.
Amendment 19, in clause 30, page 19, line 10, leave out from “add” to end of line and insert
“or remove a person or description of person”.—(Margot James.)

This amendment makes clear that regulations under Clause 30 may identify a person by describing a type of person, as well as by specifying a person.

Clause 30, as amended, ordered to stand part of the Bill.

Schedule 7 agreed to.

Clauses 31 to 34 ordered to stand part of the Bill.

**Clause 35**

THE FIRST DATA PROTECTION PRINCIPLE

Question proposed, That the clause stand part of the Bill.

Liam Byrne: Very briefly, subsection (1) includes the phrase
“must be lawful and fair”.

Could the Minister say a little more about the word “fair”? What definition is she resting on, and who is the judge of it?

Victoria Atkins: “Lawful” means any processing necessary to carry out a particular task, where that task is authorised either by statute or under common law. It would cover, for example, the taking and retention of DNA and fingerprints under the Police and Criminal Evidence Act 1984, or the police’s common law powers to disclose information required for the operation of the domestic violence disclosure scheme.

The Government recognise the importance of safeguarding sensitive personal information about individuals. Subsections (3) to (5) therefore restrict the processing of sensitive data, the definition of which includes information about an individual’s race or ethnic origin, and biometric data such as their DNA profile and fingerprints.

Further safeguards for the protection of sensitive personal data are set out in clause 42. The processing of sensitive personal data is permitted under two circumstances. The first is where the data subject has given his or her consent. The second is where the processing is strictly necessary for a law enforcement purpose and one or more of the conditions in schedule 8 to the Bill has been met. Those conditions include, for example, that the processing is necessary to protect the individual concerned or another person, or is necessary for the administration of justice. In both cases, the controller is required to have an appropriate policy document in place. We will come on to the content of such policy documents when we debate clause 42.

Liam Byrne: I am grateful for the Minister’s extensive definition, given in response to a question I did not ask. I did not ask for the definition of “lawful” but for the definition of “fair”.

Victoria Atkins: I am so sorry; I thought it was apparent from my answer. “Fair” is initially a matter for the data controller, but ultimately the Information Commissioner has oversight of these provisions and the commissioner will cover that in her guidance.

Question put and agreed to.

Clause 35 accordingly ordered to stand part of the Bill.

**Schedule 8**

CONDITIONS FOR SENSITIVE PROCESSING UNDER PART 3

Amendment made: 116, in schedule 8, page 184, line 32, at end insert—
“Safeguarding of children and of individuals at risk

3A (1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is “at risk” if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.”—(Victoria Atkins.)

Schedule 8 makes provision about the circumstances in which the processing of special categories of personal data is permitted. This amendment adds to that Schedule certain processing of personal data which is necessary for the protection of children or of adults at risk. See also Amendments 85 and 117.

Schedule 8, as amended, agreed to.

Clauses 36 to 40 ordered to stand part of the Bill.

**Clause 41**

SAFEGUARDS: ARCHIVING

Amendment made: 20, in clause 41, page 23, line 34, leave out “an individual” and insert “a data subject”.—(Victoria Atkins.)

Clause 41 makes provision about the processing of personal data for archiving purposes, for scientific or historical research purposes or for statistical purposes. This amendment aligns Clause 41(2)(b) with similar provision in Clause 19(2).

Question proposed, That the clause, as amended, stand part of the Bill.

Liam Byrne: We had a good debate on what I think was a shared objective across the Committee: to ensure that those running our big national archives—whether they are large or small organisations—should not be jeopardised by frivolous claims or, indeed, a multiplicity of claims from individuals who might seek to change the records held there in one way or another. I mentioned
to the Minister in an earlier debate that we were anxious, despite the reassurances she sought to give the Committee, that a number of organisations, including the BBC, were deeply concerned about the Bill’s impact on their work. They were not satisfied that the exemptions and safeguards in the Bill would quite do the job.

My only reason for speaking at this stage is to suggest to Ministers that if they were to have discussions with some of those organisations about possible Government amendments on Report to refine the language, and provide some of the reassurance people want, that would attract our support. We would want to have such conversations, but it would be better if the Government could find a way to come forward with refinements of their own on Report.

**Victoria Atkins:** I am happy to explore that. The reason for the clause is to enable processing to be done to create an archive for scientific or historical research, or for statistical purposes. The reason law enforcement is mentioned is that it may be necessary where a law enforcement agency needs to review historic offences, such as allegations of child sexual exploitation. I would of course be happy to discuss that with the right hon. Gentleman to see whether there are further avenues down which we should proceed.

**Liam Byrne:** I am grateful to the Minister for that response. I am happy to write to her with the representations that we have received, and perhaps she could reflect on those and write back.

**Question put and agreed to.**

**Clause 41**, as amended, accordingly ordered to stand part of the Bill.

**Clause 42**

**SAFEGUARDS: SENSITIVE PROCESSING**

Amendment made: 21, in clause 42, page 24, line 29, leave out “with the day” and insert “when”.—(Victoria Atkins.)

This amendment is consequential on Amendment 71.

Clause 42, as amended, ordered to stand part of the Bill.

Clauses 43 to 46 ordered to stand part of the Bill.

**Clause 47**

**RIGHT TO ERASURE OR RESTRICTION OF PROCESSING**

**Victoria Atkins:** I beg to move amendment 22, in clause 47, page 28, line 20, leave out second “data”.

This amendment changes a reference to a “data controller” into a reference to a “controller” (as defined in Clauses 3 and 32).

I can be brief, because this drafting amendment simply ensures that clause 47, as with the rest of the Bill, refers to a “controller” rather than a “data controller”. For the purposes of part 3, a controller is defined in clause 32(1) so it is not necessary to refer elsewhere to a “data controller”.

Amendment 22 agreed to.

Clause 47, as amended, ordered to stand part of the Bill.

Clause 48 ordered to stand part of the Bill.

---

**Clause 49**

**RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING**

**Question proposed.** That the clause stand part of the Bill.

**Liam Byrne:** We had a good debate on possible amendments to the powers of automatic decision making earlier and this is an important clause in that it creates a right not to be subject to automated decision making. Clause 49(1) states:

“A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law.”

I hope Ministers recognise that “required or authorised by law” is an incredibly broad set of questions. I would like to provoke the Minister into saying a little more about what safeguards she believes will come into place to ensure that decisions are not taken that jeopardise somebody’s human rights and their right to appeal and justice based on those human rights. It could be that the Minister decides to answer those questions in the debate on clause 50, but it would be useful for her to say a little more about her understanding of the phrase “significant decision” and a little more about what kind of safeguards will be needed to ensure that decisions that are cast in such a broad way do not impact on people in a negative way.

**Victoria Atkins:** Clause 49 establishes the right for individuals not to be subject to a decision based exclusively on automated processing, where that decision has an adverse impact on the individual. It is important to protect that right to enhance confidence in law enforcement processing and safeguard individuals against the risk that a potentially damaging decision is taken without human intervention. The right hon. Gentleman asked about the definition of a significant decision. It is set out in the Bill.

We are not aware of any examples of the police solely using automated decision-making methods, but there may be examples in other competent authorities. The law enforcement directive includes that requirement, so we want to transpose it faithfully into statute, and we believe we have captured the spirit of the requirement.

3 pm

**Louise Haigh:** There is the example of Durham police force—an excellent police force in many regards—using automated decision making to decide who does and does not remain in custody, and when people receive their charge. A human is involved in that decision-making process at the moment, but the Bill would enable that to be taken away and allow it to be done purely on an automated basis. I am sure the Minister understands our concerns about removing humans from that decision-making process.

**Victoria Atkins:** I have to say that I am not familiar with that example. I look to my officials—

**The Chair:** Order. The hon. Lady has on a number of occasions referred to her officials. She should remember at all times that, as far as the Committee is concerned, there are no officials in this room, even though self-evidently there are.
Victoria Atkins: I wonder whether that is captured in the spirit of the Bill. Forgive me, Mr Hanson. This is my first Bill Committee as a Minister and I was not aware of that. Many apologies.

I am not familiar with that example. It would be a very interesting exercise under the PACE custody arrangements. I will look into it in due course. These protections transpose the law enforcement directive, and we are confident that they meet those requirements.

Question put and agreed to.

Clause 49 accordingly ordered to stand part of the Bill.

Clause 50

Automated decision-making authorised by law: safeguards

Amendments made: 23, in clause 50, page 30, line 11, leave out “21 days” and insert “1 month”.

Clause 50(2)(b) provides that where a controller notifies a data subject under Clause 50(2)(a) that the controller has taken a "qualifying significant decision" in relation to the data subject based solely on automated processing, the data subject has 21 days to request the controller to reconsider or take a new decision not based solely on automated processing. This amendment extends that period to one month.

Amendment 24, in clause 50, page 30, line 17, leave out “21 days” and insert “1 month”.—(Victoria Atkins.)

Clause 50(3) provides that where a data subject makes a request to a controller under Clause 50(2)(b) to reconsider or retest a decision based solely on automated processing, the controller has 21 days to respond. This amendment extends that period to one month.

Question proposed, That the clause, as amended, stand part of the Bill.

Liam Byrne: I remain concerned that the safeguards the Government have proposed to ensure people’s human rights are not jeopardised by the use of automated decision making are, frankly, not worth the paper they are written on. We know that prospective employers and their agents use algorithms and automated systems to analyse very large sets of data and, through the use of artificial intelligence and machine learning, make inferences about whether people are appropriate to be considered to be hired or retained by a particular company. We have had a pretty lively debate in this country about the definition of a worker, and we are all very grateful to Matthew Taylor for his work on that question. Some differences emerged, and the Business, Energy and Industrial Strategy Committee has put its views on the record.

The challenge is that our current labour laws, which were often drafted decades ago, such as the Sex Discrimination Act 1975 and the Race Relations Act 1965, are no longer adequate to protect people in this new world, in which employers are able to use such large and powerful tools for gathering and analysing data, and making decisions.

We know that there are problems. We already know that recruiters use Facebook to seek candidates in a way that routinely discriminates against older workers by targeting job advertisements. That is not a trivial issue; it is being litigated in the United States. In the United Kingdom, research by Slater and Gordon, a group of employment lawyers, found that one in five bosses who had access to profiling tools admitted to using them to actively seek out people based on criteria such as age, gender and race. Female Uber drivers earn 7% less than men when pay is determined by algorithms. A number of practices in the labour market are disturbing and worrying, and they should trouble all of us.

The challenge is that clause 50 needs to include a much more comprehensive set of rights and safeguards. It should clarify that the Equality Act 2010 and protection from discrimination applies to all new forms of decision making that engage core labour rights around recruitment, terms of work or dismissal. There should be new rights about algorithmic fairness at work to ensure equal treatment where an algorithm or automated system takes a decision that impinges on someone’s rights. There should be a right to explanation where significant decisions are taken based on an algorithm or an automated decision. There is also a strong case to create a duty on employers, if they are a large organisation, to undertake impact assessments to check whether they are, often unwittingly, discriminating against people in a way that we think is wrong.

Over the last couple of weeks, we have seen real progress in the debate about gender inequalities in pay. Many of us will have looked in horror at some of the news that emerged from the BBC and at some of the evidence that emerged from ITV and The Guardian. We have to contend with the reality that automated decision-making processes are under way in the labour market that could make inequality worse rather than better. The safeguards that we have in clause 50 do not seem up to the job.

I hope the Minister will say a bit more about the problems that she sees with future algorithmic decision making. I am slightly troubled that she is unaware of some live examples in the Home Office space in one of our most successful police forces, and there are other examples that we know about. Perhaps the Minister might say more about how she intends to improve the Bill with regard to that issue between now and Report.

Victoria Atkins: I will pick up on the comments by the right hon. Gentleman, if I may.

In the Durham example given by the hon. Member for Sheffield, Heeley, I do not understand how a custody sergeant could sign a custody record without there being any human interaction in that decision-making process. A custody sergeant has to sign a custody record and to review the health of the detainee and whether they have had their PACE rights. I did not go into any details about it, because I was surprised that such a situation could emerge. I do not see how a custody sergeant could be discharging their duties under the Police and Criminal Evidence Act 1984 if their decision as to custody was based solely on algorithms, because a custody record has to be entered.

Louise Haigh: I thank the Minister for allowing me to clarify. I did not say that it was solely an algorithmic decision already. Durham is using an algorithm known as the harm assessment risk tool. A human makes a decision based on the algorithm’s recommendations. The point I was making was that law enforcement is using algorithms to make very important decisions that limit an individual’s right to freedom, let alone the right to privacy or anything else, but the Bill will enable law
enforcement to take that further. I appreciate what the Minister is saying about PACE and the need for a custody sergeant, but the Bill will enable law enforcement to take that further and to remove the human right—

Victoria Atkins: This has been a moment of genuine misunderstanding. Given how the hon. Lady presented that, to me it sounded as if she was saying that the custody record and the custody arrangements of a suspect—detaining people against their will in a police cell—was being done completely by a computer. That was how it sounded. There was obviously an area of genuine misunderstanding, so I am grateful that she clarified it. She intervened on me when I said that we were not aware of any examples of the police solely using automated decision making—that is when she intervened, but that is not what she has described. A human being, a custody sergeant, still has to sign the record and review the risk assessment to which the hon. Lady referred. The police are using many such examples nowadays, but the fact is that a human being is still involved in the decision-making process, even in the issuing of penalties for speeding. Speeding penalties may be automated processes, but there is a meaningful element of human review and decision making, just as there is with the custody record example she gave.

There was a genuine misunderstanding there, but I am relieved, frankly, given that the right hon. Member for Sheffield, Heeley made when I was talking about any examples of the police solely using automated decision making.

Liam Byrne: Will the Minister give way?

Victoria Atkins: No, with respect—

Liam Byrne: This is a Bill Committee, line-by-line scrutiny.

Victoria Atkins: Line-by-line scrutiny, but I was acting in good faith on an intervention that the hon. Member for Sheffield, Heeley made when I was talking about any examples of the police solely using automated decision making.

Liam Byrne: On a point of order, Mr Hanson.

The Chair: I hope it is, Mr Byrne.

Liam Byrne: May I ask for your guidance on this question? We are in a Bill Committee that is tasked with scrutinising the Bill line by line. Is it customary for Ministers to refuse to give way on a matter of detail?

The Chair: Ultimately, whether the Minister gives way is a matter for the Minister—that is true for any Member who has the Floor—but it is normal practice to debate aspects of legislation thoroughly. Ultimately, however, it remains the choice of the Minister or any other Member with the Floor whether to give way.

Victoria Atkins: I think it is fair to say that I have given way on interventions, but the right hon. Gentleman seemed to be seeking to argue with me as to my understanding of what his colleague, the hon. Member for Sheffield, Heeley, had said. Frankly, that is a matter for me to understand.

The Chair: Order. We are debating clause 50 of the Bill, so may I suggest that in all parts of the Committee we focus our minds on the clause?

Victoria Atkins: I am grateful—

Liam Byrne: Will the Minister give way on that point?

Victoria Atkins: I have lost track of which point the right hon. Gentleman wants me to give way on.

Liam Byrne: Let me remind the Minister. What we are concerned about on the question of law enforcement is whether safeguards that are in place will be removed under the Bill. That is part and parcel of a broader debate that we are having about whether the safeguards that are in the Bill will be adequate. So let me return to the point I made earlier to the Minister, which is that we would like her reflections on what additional safeguards can be drafted into clauses 50 and 51 before Report stage.

Victoria Atkins: Clause 49 is clear that individuals should not be subject to a decision based solely on automated processing if that decision significantly or adversely has an impact on them, legally or otherwise, unless required by law. If that decision is required by law, clause 50 specifies the safeguards that controllers should apply to ensure that the impact on the individual is minimised. Critically, that includes informing the data subject that a decision has been taken and giving that individual 21 days in which to ask the controller to reconsider the decision, or to retake the decision with human intervention.

A point was made about the difference between automated processing and automated decision making. Automated processing is when an operation is carried out on personal data using predetermined fixed parameters that allow for no discretion by the system and do not involve further human intervention in the operation to produce a result or output. Such processing is used regularly in law enforcement to filter large datasets down to manageable amounts for a human operator to use. Automated decision making is a form of automated processing that allows the system to use discretion, potentially based on algorithms, and requires the final decision to be made without human interference. The Bill seeks to clarify that, and the safeguards are set out in clause 50.

Question put and agreed to.

Clause 50, as amended, accordingly ordered to stand part of the Bill.

Clause 51

EXERCISE OF RIGHTS THROUGH THE COMMISSIONER

3.15 pm

Victoria Atkins: I beg to move amendment 25, in clause 51, page 31, line 2, leave out from first “the” to end of line 3 and insert

“restriction imposed by the controller was lawful;”.

This amendment changes the nature of the request that a data subject may make to the Commissioner in cases where rights to information are restricted under Clause 44(4) or 45(4). The effect is that a data subject will be able to request the Commissioner to check that the restriction was lawful.
The Chair: With this it will be convenient to discuss Government amendment 26.

Victoria Atkins: These technical amendments are required to ensure that the provisions in clause 51 do not inadvertently undermine criminal investigations by the police or other competent authorities. Under the Bill, where a person makes a subject access request, it may be necessary for the police or other competent authority to give a “neither confirm nor deny” response, for example in order to avoid tipping someone off that they are under investigation for a criminal offence. In such a case, the data subject may exercise their rights under clause 51 to ask the Information Commissioner to check that the processing of their personal data complies with the provisions in part 3. It would clearly undermine a “neither confirm nor deny” response to a subject access request if a data subject could use the provisions in part 3 to secure confirmation that the police were indeed processing their information.

It is appropriate that the clause focuses on the restriction of a data subject’s rights, not on the underlying processing. The amendments therefore change the nature of the request that a data subject may make to the commissioner in cases where rights to information are restricted under clause 44(4) or clause 45(4). The effect of the amendments is that a data subject will be able to ask the commissioner to check that the restriction was lawful. The commissioner will then be able to respond to the data subject in a way that does not undermine the original “neither confirm nor deny” response.

Liam Byrne: This is a significant amendment—I understand the ambition behind the clause—so it is worth dwelling on it for a moment. I would like to check my understanding of what the Minister said. In a sense, if an investigation is under way and the individual under investigation makes a subject access request to the police and gets a “neither confirm nor deny” response, the data subject will be able to ask the Information Commissioner to investigate. Will the Minister say a little more about what message will go from the Information Commissioner to the data subject. Will that be a standard message that will go from the Information Commissioner to the data subject. Will that be a standard message? Will it be in any way detailed? Will it reflect in any way on the information that the police provide? Or will it simply be a blank message such as “I, the Information Commissioner, am satisfied that your information has been processed lawfully”? I do not think the Information Commissioner is likely to ask for too much detail about the nature of the offence, but she will obviously ask whether data has been processed lawfully. She will want to make checks in that way. Unless the Information Commissioner is able to provide some kind of satisfactory response to the person who has made the original request, we will end up with an awful administrative muddle that will take of lot of the courts’ time. Perhaps the Minister could put our minds at rest on that.

Victoria Atkins: The Information Commissioner will get the information but, by definition, she does not give that information to the subject, because law enforcement will have decided that it meets the criteria for giving a “neither confirm nor deny” response from their perspective. The commissioner then looks at the lawfulness of that; if she considers it to be lawful, she will give the same response—that the processing meets part 3 obligations.

Amendment 25 agreed to.

Amendment made: 26, in clause 51, page 31, line 11, leave out from first “the” to end of line 12 and insert “restriction imposed by the controller was lawful.”—(Victoria Atkins.)

This amendment is consequential on Amendment 25.

Clause 51, as amended, ordered to stand part of the Bill.

Clause 52 ordered to stand part of the Bill.

Clause 53

MANIFESTLY UNFOUNDED OR EXCESSIVE REQUESTS BY THE DATA SUBJECT

Amendments made: 27, in clause 53, page 31, line 39, leave out “or 47” and insert “47 or 50”.

Clause 53(1) provides that where a request from a data subject under Clause 45, 46 or 47 is manifestly unfounded or excessive, the controller may charge a reasonable fee for dealing with the request or refuse to act on the request. This amendment applies Clause 53(1) to requests under Clause 50 (automated decision making). See also Amendment 28.

Amendment 28, in clause 53, page 32, line 4, leave out “or 47” and insert “47 or 50”.—(Victoria Atkins.)

Clause 53(3) provides that where there is an issue as to whether a request under Clause 45, 46 or 47 is manifestly unfounded or excessive, it is for the controller to show that it is. This amendment applies Clause 53(3) to requests under Clause 50 (automated decision making). See also Amendment 27.

Question proposed, That the clause, as amended, stand part of the Bill.

Liam Byrne: We have just agreed a set of amendments that, on the face of it, look nice and reasonable. We can all recognise the sin that the Government are taking aim at, and that the workload of the Information Commissioner’s Office and of others has to be kept under control, so we all want to deter tons of frivolous and meaningless requests. None the less, a lot of us have noticed that, for example, the introduction of fees for industrial tribunals makes it a lot harder for our constituents to secure justice.
I wonder, having now moved the amendment successfully, whether the Minister might tell us a little more about what will constitute a reasonable fee and what will happen to those fees. Does she see any relationship between the fees being delivered to her Majesty’s Government and the budget that is made available for the Information Commissioner? Many of us are frankly worried, given the new obligations of the Information Commissioner, about the budget she has to operate with and the resources at her disposal. Could she say a little more, to put our minds at rest, and reassure us that these fees will not be extortionate? Where sensible fees are levied, is there some kind of relationship with the budget that the Information Commissioner might enjoy?

Victoria Atkins: Clause 35 establishes the principle that subject access requests should be provided free of charge in most cases. That will be the default position in most cases. In terms of the fees, that will not be a matter to place in statute; certainly, I can write to the right hon. Gentleman with my thoughts on how that may develop. The intention is that in the majority of cases, there will be no charge.

Question put and agreed to.
Clause 53, as amended, accordingly ordered to stand part of the Bill.

Clause 54

MEANING OF “APPLICABLE TIME PERIOD”

Amendments made: 29, in clause 54, page 32, line 14, leave out “day” and insert “time”.
This amendment is consequential on Amendment 71.
Amendment 30, in clause 54, page 32, line 15, leave out “day” and insert “time”.—(Victoria Atkins.)
This amendment is consequential on Amendment 71.
Clause 54, as amended, ordered to stand part of the Bill.

Clauses 55 to 63 ordered to stand part of the Bill.

Clause 64

DATA PROTECTION IMPACT ASSESSMENT

Louise Haigh: I beg to move amendment 142, in clause 64, page 37, line 2, leave out “is likely to” and insert “may”.

The Chair: With this it will be convenient to discuss the following:
Amendment 143, in clause 64, page 37, line 2, leave out “high”.
Amendment 144, in clause 64, page 37, line 15, leave out “is likely to” and insert “may”.
Amendment 145, in clause 64, page 37, line 15, leave out “high”.
Amendment 146, in clause 65, page 37, line 19, leave out subsection (1) and insert—
“(1) This section applies where a controller intends to—
(a) create a filing system and process personal data forming part of it, or
(b) use new technical or organisational measures to acquire, store or otherwise process personal data.”
Amendment 147, in clause 65, page 37, line 23, leave out “would” and insert “could”.

Amendment 148, in clause 65, page 37, line 23, leave out “high”.
Amendment 149, in clause 65, page 37, line 44, at end insert—
“(8) If the Commissioner is not satisfied that the controller or processor (where the controller is using a processor) has taken sufficient steps to remedy the failing in respect of which the Commissioner gave advice under subsection (4), the Commissioner may exercise powers of enforcement available to the Commissioner under Part 6 of this Act.”

New clause 3—DATA PROTECTION IMPACT ASSESSMENT: INTELLIGENCE SERVICES PROCESSING—
“(1) Where a type of processing proposed under section 103(1) may result in a risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.
(2) A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.
(3) A data protection impact assessment must include the following—
(a) a general description of the envisaged processing operations;
(b) an assessment of the risks to the rights and freedoms of data subjects;
(c) the measures envisaged to address those risks;
(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.
(4) In deciding whether a type of processing could result in a risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing.”

New clause 4—PRIOR CONSULTATION WITH THE COMMISSIONER: INTELLIGENCE SERVICES PROCESSING—
“(1) This section applies where a controller proposes that a particular type of processing of personal data be carried out under section 103(1).
(2) The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section [Data protection impact assessment: intelligence services processing] indicates that the processing of the data could result in a risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk).
(3) Where the controller is required to consult the Commissioner under subsection (2), the controller must give the Commissioner—
(a) the data protection impact assessment prepared under section [Data protection impact assessment: intelligence services processing], and
(b) any other information requested by the Commissioner to enable the Commissioner to make an assessment of the compliance of the processing with the requirements of this Part.
(4) Where the Commissioner is of the opinion that the intended processing referred to in subsection (1) would infringe any provision of this Part, the Commissioner must provide written advice to the controller and, where the controller is using a processor, to the processor.
(5) The written advice must be provided before the end of the period of 6 weeks beginning with receipt of the request for consultation by the controller or the processor.
(6) The Commissioner may extend the period of 6 weeks by a further period of one month, taking into account the complexity of the intended processing.
(7) If the Commissioner extends the period of 6 weeks, the Commissioner must—
Cameras. As a result, the surveillance camera code of practice was introduced to regulate overt public space surveillance through facial recognition. The Protection of Freedoms Act 2012, in particular when policing large events, has been trialled for three years. I suggest that it is being trialled by the Metropolitan police, but it has not been adequately designed to strengthen the requirement to conduct impact assessments, and to require permission from the Information Commissioner for the purposes of data processing for law enforcement agencies. Impact assessments are a critical feature of the landscape of data protection, particularly where new technology has evolved. It is vital that we have in place enabling legislation and protective legislation to cover new technologies and new methods of data collection and processing.

Since the introduction of the Data Protection Act 1998, the advance of technology has considerably increased the ability of organisations to collect data, as we have discussed. The impact assessment as envisaged allows for an assessment to be conducted where there are systematic and extensive processing activities, including profiling, and where decisions have legal effects, or similarly significant effects, on individuals. In addition, an assessment can be conducted where there is large-scale processing of special categories of data, or personal data in relation to criminal convictions or offences, and where there is a high risk to rights and freedoms—for example, based on the sensitivity of the processing activity.

Given the breadth and reach of new technology, it is right that impact assessments are conducted where the new technology may present a risk, rather than a “high risk”, as envisaged in the Bill. That is what we seek to achieve with the amendments. New technology in law enforcement presents a unique challenge to the data protection and processing environment. The trialling of technology, including facial recognition and risk assessment algorithms, as already discussed, has not been adequately considered by Parliament to date, nor does it sit easily within the current legal framework. I do not doubt that such technologies have a significant role to play in making law enforcement more effective and efficient, but they have to be properly considered by Parliament, and they need to have adequate oversight to manage their appropriate use.

Facial recognition surveillance was mentioned in Committee on Tuesday. The Minister was right to say that it is being trialled by the Metropolitan police, but it has been trialled for three years running. I suggest that it is no longer a trial. It is also being used by South Wales police and other police forces across the country, particularly when policing large events. The Metropolitan police use it in particular for Notting Hill carnival.

In September last year, the Policing Minister made it clear in response to a written question that there is no legislation regulating the use of CCTV cameras with facial recognition. The Protection of Freedoms Act 2012 introduced the regulation of overt public space surveillance cameras. As a result, the surveillance camera code of

Louise Haigh: The amendments in my name, and in the names of my right hon. and hon. Friends, are all designed to strengthen the requirement to conduct impact assessments, and to require permission from the Information Commissioner for the purposes of data processing for law enforcement agencies. Impact assessments are a critical feature of the landscape of data protection, particularly where new technology has evolved. It is vital that we have in place enabling legislation and protective legislation to cover new technologies and new methods of data collection and processing.

Since the introduction of the Data Protection Act 1998, the advance of technology has considerably increased the ability of organisations to collect data, as we have discussed. The impact assessment as envisaged allows for an assessment to be conducted where there are systematic and extensive processing activities, including profiling, and where decisions have legal effects, or similarly significant effects, on individuals. In addition, an assessment can be conducted where there is large-scale processing of special categories of data, or personal data in relation to criminal convictions or offences, and where there is a high risk to rights and freedoms—for example, based on the sensitivity of the processing activity.

Given the breadth and reach of new technology, it is right that impact assessments are conducted where the new technology may present a risk, rather than a “high risk”, as envisaged in the Bill. That is what we seek to achieve with the amendments. New technology in law enforcement presents a unique challenge to the data protection and processing environment. The trialling of technology, including facial recognition and risk assessment algorithms, as already discussed, has not been adequately considered by Parliament to date, nor does it sit easily within the current legal framework. I do not doubt that such technologies have a significant role to play in making law enforcement more effective and efficient, but they have to be properly considered by Parliament, and they need to have adequate oversight to manage their appropriate use.

Facial recognition surveillance was mentioned in Committee on Tuesday. The Minister was right to say that it is being trialled by the Metropolitan police, but it has been trialled for three years running. I suggest that it is no longer a trial. It is also being used by South Wales police and other police forces across the country, particularly when policing large events. The Metropolitan police use it in particular for Notting Hill carnival.

In September last year, the Policing Minister made it clear in response to a written question that there is no legislation regulating the use of CCTV cameras with facial recognition. The Protection of Freedoms Act 2012 introduced the regulation of overt public space surveillance cameras. As a result, the surveillance camera code of practice was introduced by the Secretary of State in 2013. However, there is no reference to facial recognition in the Act, even though it provides the statutory basis for public space surveillance cameras.

Neither House of Parliament has ever considered or scrutinised automated facial recognition technology. To do so after its deployment—after three years of so-called trialling by the Metropolitan police—is unacceptable, particularly given the technology’s significant and unique impact on rights. The surveillance camera commissioner has noted that “clarity regarding regulatory responsibility” for such facial recognition software is “an emerging issue”. We urgently need clarity on whether the biometric commissioner, the Information Commissioner or the surveillance camera commissioner has responsibility for this use of technology. Our amendments suggest that the Information Commissioner should have scrutiny powers over this, but if the Minister wants to tell me that it should be any of the others, we will be happy to support that.

3.30 pm

Clearly, there needs to be some scrutiny of this very important and invasive technology, which provides recommendations to law enforcement agencies to act, to stop and search and, potentially, to detain people. There are still no answers as to what databases law enforcement agencies are matching faces against, what purposes the technology can and cannot be used for, what images are captured and stored, who can access those images and how long they are stored for.

In 2013, the Government said that the Home Office would publish a forensics and biometrics strategy. Five years on, that strategy has still not been published. The deadline has been missed by quite some time. I appreciate that they have said that they will publish it by June 2018, but in the meantime many of these emerging technologies are being used with absolutely no oversight and, as the Minister said, no legal basis. That simply cannot be acceptable.

There are other issues with the use of facial recognition technology. It is used extensively in the United States, and several studies have found that commercial facial recognition algorithms have in-built biases and issues around demographic accuracy. In particular, they are more likely to misidentify women and black people. That might be because of bias encoded into the software by programmers, or it might be because of an underrepresentation of people from black and minority ethnic backgrounds and women in the training datasets. Either way, the technology that the police are currently using in this country has not been tested against such biases.

Surely that testing is urgently needed when we consider the issues that the Home Secretary and the Prime Minister have tried to tackle around the disproportionate use of stop-and-search powers against black and minority ethnic populations, and the issues around trust in the police that that has engendered. Why are we not concerned about the same issues with this very invasive technology that could recreate those exact same biases?

The facial recognition software used by the South Wales police has not been tested against those biases either, but this is not just about facial recognition software. Significant technologies and algorithms are being used by law enforcement agencies across the country. We have already discussed the algorithm used to make
recommendations on custody. Automatic number plate recognition has been rolled out across many forces—we will discuss a code of practice for that when we come to a later amendment. Fingerprint-scanning mobile devices have recently been rolled out across West Yorkshire police. I mentioned earlier, in relation to another amendment, that South Yorkshire police is now tagging individuals who frequently go missing.

It was brought to my attention this morning that South Yorkshire police and Avon and Somerset police have a technology that allows them to track the movements of mobile phone users within a given area and intercept texts and calls. These are called international mobile subscriber identity—IMSI—catchers. They mimic cell towers, which mobile phones connect to in order to make and receive phone calls and text messages. When they are deployed, every mobile phone within an 8 sq km area will try to connect to the dummy tower. The IMSI catchers will then trace the location and unique IMSI number of each phone, which can then be used to identify and track people.

Those are all worrying invasions into the privacy of individuals who have not been identified by the police as being about to commit criminal activity, nor are wanted by the police or law enforcement agencies. In that last example, they are just people who happen to be within the 8 sq km area in which the police would like to track and intercept people’s phones.

It may be that every one of those technologies is being used proportionately and necessarily, and that we would all be happy about the way that they are being used. However, if there is no basis in law and no commissioner overseeing the use of these technologies, and if Parliament has never discussed them, surely this is the opportunity to ensure that that happens, to give people confidence that the police and other enforcement agencies will be using them proportionately and not excessively.

Furthermore, the police national database currently contains over 21 million images of individuals, over 9 million of whom have never been charged or convicted of any offence. The biometrics commissioner has already said that it is completely unacceptable for the Home Office to retain those images when it has no good reason to do so. Doing so would also be a clear breach of clause 47, which covers the right to erasure, when there is no reasonable need for the police national database to contain those images. That raises issues around facial recognition software, because if we are matching people’s faces against a database where there is no legal right for those faces to be held, that would already be a breach of the Bill as un-amended.

I hope the Minister will accept that there are good reasons for these amendments or, if she can, assure me that these existing and emerging technologies will be covered by the Bill, and that a relevant commissioner will oversee this, both before any technology or new method of data collection and data processing is rolled out by law enforcement, and afterwards, when an individual’s data rights have been potentially abused. We need clear principles around what purposes any of these technologies can or cannot be used for, what data is captured and stored, who can access that data, how long it is stored for and when it is deleted. I am not convinced that the Bill as it stands protects those principles.

**Liam Byrne:** I rise briefly to support my hon. Friend’s excellent speech. The ambition of Opposition Members on the Committee is to ensure that the Government have in place a strong and stable framework for data protection over the coming years. Each of us, at different times in our constituencies, have had the frustration of working with either local police or their partners and bumping into bits of regulation or various procedures that we think inhibit them from doing their job. We know that at the moment there is a rapid transformation of policing methods. We know that the police have been forced into that position, because of the pressure on their resources. We know that there are police forces around the world beginning to trial what is sometimes called predictive policing or predictive public services, whereby, through analysis of significant data patterns, they can proactively deploy police in a particular way and at a particular time. All these things have a good chance of making our country safer, bringing down the rate of crime and increasing the level of justice in our country.

The risk is that if the police lack a good, clear legal framework that is simple and easy to use, very often sensible police, and in particular nervous and cautious police and crime commissioners, will err on the side of caution and actually prohibit a particular kind of operational innovation, because they think the law is too muddy, complex and prone to a risk of challenge. My hon. Friend has given a number of really good examples. The automatic number plate recognition database is another good example of mass data collection and storage in a way that is not especially legal, and where we have waited an awfully long time for even something as simple as a code of practice that might actually put the process and the practice on a more sustainable footing. Unless the Government take on board my hon. Friend’s proposed amendments, we will be shackling the police, stopping them from embarking on many of the operational innovations that they need to start getting into if they are to do their job in keeping us safe.

**Stuart C. McDonald** (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): I will speak briefly in support of amendments 142 to 149, as well as new clauses 3 and 4. As it stands, clause 64 requires law enforcement data controllers to undertake a data protection impact assessment if “a type of processing is likely to result in a high risk to the rights and freedoms of individuals”. That assessment would look at the impact of the envisaged processing operations on the protection of personal data and at the degree of risk, measures to address those risks and possible safeguards. If the impact assessment showed a high risk, the controller would have to consult the commissioner under clause 65.

It is important to be clear that the assessment relates to a type of processing. Nobody is asking anyone to undertake an impact assessment every time the processing occurs. With that in mind, the lower threshold for undertaking an assessment suggested in the amendments seems appropriate. We should be guarding not just against probable or high risks, but against any real risk. The worry is that if we do not put these tests in place, new forms of processing are not going to be appropriately scrutinised. We have had the example of facial recognition technology, which is an appropriate one.

New clauses 3 and 4 do a similar job for the intelligence services in part 4, so they also have our support.
Darren Jones: I rise to support the amendments in the name of my hon. Friend the Member for Sheffield, Heeley. I had the pleasure of cross-examining Baroness Williams of Trafford, who is the Minister responsible for some of these issues, on the Select Committee on Science and Technology in our inquiry on the biometric strategy and why there has been such a delay in the Government publishing that document. We had grave concerns about the delay in the strategy, but also about the way in which IT systems and servers in different forces act in different ways, which make things potentially very difficult.

The amendments would add safeguards to legitimate purposes—to prevent them from going too far. They should be welcomed by the Government and included in the Bill. There are a number of situations where, in this developing area of technology, which could be very useful to us as a country, as my hon. Friends have said, we need to ensure that the appropriate safeguards are in place. On facial recognition, we know from information received by the Science and Technology Committee that there is too high a number of facial records on the police national database and other law enforcement databases, when there is no legitimate reason for them to be there. We understand that it is difficult to delete them, but that is, with respect, not a good enough answer.

The Select Committee also heard—I think I mentioned this in an earlier sitting—that we have to be careful about the data that the Government hold. The majority of the adult population already has their facial data on Government databases, in the form of passport and driving licence imagery. When we start talking about the exemptions to being able to share data between different Government functions and law enforcement functions, and the exemptions on top of that for the ability to use those things, we just need to be careful that it does not get ahead of us. I know it is difficult to legislate perfectly for the future, but these safeguards would help to make it a safer place.

I will mention briefly the IMSI-catchers, because that covers my constituency of Bristol North West. It was the Bristol Cable, a local media co-operative of which I am a proud member—I pay £1 a month, so I declare an interest. The Select Committee on Science and Technology in our inquiry on the biometric strategy and why there has been such a delay in the Government publishing that document. We had grave concerns about the delay in the strategy, but also about the way in which IT systems and servers in different forces act in different ways, which make things potentially very difficult.

In a situation where human resource is extremely stretched, such as in the police service, the tendency will understandably be to rely on the decisions of the systems within the frameworks that are provided, because there is not time to do full human intervention properly. That is why the safeguards are so important—to prevent things getting ahead of us. I hope the Government support the amendments, which I think are perfectly sensible.

Victoria Atkins: I have just a small correction. The hon. Member for Sheffield, Heeley said in error that the Home Office were holding on to the photographs. It is not the Home Office. It is individual police forces that hold that.

Louise Haigh: No, it is on the police national computer. That falls under the responsibility of the Home Office, not individual forces.

Victoria Atkins: That is run by the police. I do not want the misapprehension to be established that there is an office in the Home Office in Marsham Street where these photographs are held on a computer. It is on the police national computer, which is a secure system that people have to have security clearance to get into. It is not completely accurate to say that the Home Office has possession of it.

3.45 pm

I want to reassure the hon. Lady, because the picture she painted of the various systems she described was that they are unregulated, but that is not the case. Where they involve the processing of personal data, they will be caught by the Bill and the 1998 Act. Other statutory provisions may also apply—for example, the provisions of PACE relating to biometric information—and the surveillance camera commissioner will have a role in relevant cases. Facial recognition systems, in particular, are covered by the 1998 Act and the Bill, because they relate to personal data. Any new systems that are developed will be subject to a data protection impact assessment.

Law enforcement processing of ANPR data for the purpose of preventing, detecting, investigating and prosecuting crime will be conducted under part 3 of the Bill. When the data is processed by other organisations for non-law enforcement purposes, such as the monitoring of traffic flows, the data will be processed under part 2 of the Bill.

Part 3 of the Bill puts data protection impact assessments on a statutory footing for the first time. The purpose of such impact assessments is to prompt a controller to take action and put in place safeguards to mitigate the risk to individuals in cases in which processing is likely to result in a high risk to the rights and freedoms of their personal data. For example, under clause 64 the police will be required to carry out a data protection impact assessment before the new law enforcement data service—the next-generation police national computer—goes live. Clauses 64 and 65 faithfully transpose the provisions of PACE relating to biometric information and the surveillance camera commissioner will have a role in relevant cases. Facial recognition systems, in particular, are covered by the 1998 Act and the Bill, because they relate to personal data. Any new systems that are developed will be subject to a data protection impact assessment.

Law enforcement processing of ANPR data for the purpose of preventing, detecting, investigating and prosecuting crime will be conducted under part 3 of the Bill. When the data is processed by other organisations for non-law enforcement purposes, such as the monitoring of traffic flows, the data will be processed under part 2 of the Bill.

Part 3 of the Bill puts data protection impact assessments on a statutory footing for the first time. The purpose of such impact assessments is to prompt a controller to take action and put in place safeguards to mitigate the risk to individuals in cases in which processing is likely to result in a high risk to the rights and freedoms of their personal data. For example, under clause 64 the police will be required to carry out a data protection impact assessment before the new law enforcement data service—the next-generation police national computer—goes live. Clauses 64 and 65 faithfully transpose the provisions of the law enforcement directive, and the provisions in part 4 faithfully give effect to draft Council of Europe convention 108.

Amendments 142 to 145 would extend the scope of the requirements in clause 64 so that a formal impact assessment would have to be carried out irrespective of the likelihood or significance of the risk. That would place overly burdensome duties on controllers and their resources, with limited benefit to the data subject.

Louise Haigh: I would be grateful if the Minister can confirm that all the examples we raised today will fall under the “high risk” category in the Bill.

Victoria Atkins: I will deal with the definition of high risk in a moment. Clause 64 separates out the processing most likely significantly to affect an individual’s rights and freedom, which requires an additional level of
assessment to reflect the higher risk. The amendments would water down the importance of those assessments. That is not to say that consideration of the impact on rights and freedoms can be overlooked. It will, of course, remain necessary for the controller to carry out that initial assessment to determine whether a full impact assessment is required. Good data protection is not achieved by putting barriers in the way of processing. It is about considering the risk intelligently and applying appropriate assessments accordingly.

On the question of high risk, officers or data controllers will go through that process when considering whether a data protection impact assessment is correct. I will write to the hon. Lady to clarify whether the bodies and lists she mentioned will be defined as high risk. The fact is that they are none the less regulated by various organisations.

Matt Warman: The crucial point—I do not think the Opposition disagree with it—is that, although some things contain an element of risk, there are also huge benefits. Surely nobody wishes to do anything that prevents law enforcement from using hugely advantageous new technology, which will allow it to divert its resources to even more valuable areas.

Victoria Atkins: Indeed. A pertinent example of that is the development of artificial intelligence to help the police categorise images of child sexual exploitation online. That tool will help given the volume of offences now being carried out across the world. It will also help the officers involved in those cases, because having to sit at a computer screen and categorise some of these images is soul-breaking, frankly. If we can use modern technology and artificial intelligence to help categorise those images, that must surely be a good thing.

Louise Haigh: There is absolutely no argument over that. As a former special constable myself, I have no wish to put obstacles in the way of law enforcement. There is a particular need to develop technology to help digital investigations, and I think the Government have been delaying that. Human failures in those investigations have led to the collapse of several trials over the past couple of months.

The Minister says that the surveillance camera commissioner has a role. The commissioner has said that there needs to be further clarity on regulatory responsibility. It is not clear whether it is the surveillance camera commissioner, the biometrics commissioner or the Information Commissioner who has responsibility for facial recognition software. Does she accept that the Government urgently need to provide clarity, as well as guidance to the National Police Chiefs Council and police forces, about the use of this potentially invasive software?

Victoria Atkins: Specifically on clause 64, which is about the data protection impact assessment, the judgment as to whether the proposed processing is high risk must be a matter for the controller. On the face of it, many of the systems that the hon. Lady described in her speech will involve high risk, but with respect the decision is not for me to make as a Minister on my feet in Committee. We must allow data controllers the freedom and responsibility to make those assessments. They are the ones that make the decisions and what flows from that in terms of processing.

If the hon. Lady will write to me on the more general, wider point about oversight of the surveillance camera commissioner and so on, I would be happy to take that up outside of Committee.

Louise Haigh: The issue about whether it is high risk is of course a matter for the data controller, but we are scrutinising this Bill, and the Minister is asking us to support a test of high risk. I am sure the whole Committee would agree that all the cases that have been suggested today involve an incredibly high risk. They involve deprivation of liberty and invasion of privacy. The idea that we would accept a definition of high risk that does not cover those examples is too much for the Opposition to support. That is why the amendment exists. We need to test exactly what the Government envisage in the definition of high risk.

Victoria Atkins: May I just clarify whether the hon. Lady intends to amend her amendment to list the various categories she listed in her speech? I have been very clear that high risk is defined as including processing where there is a particular likelihood of prejudice to the rights and freedoms of data subjects. I would be very cautious about listing examples in the Bill through an amendment, because as we have all acknowledged, criminality and other things develop over time. It would be very bold to put those categories in the Bill.

Louise Haigh: No one is suggesting that such examples should go in the Bill. I appreciate this is the Minister’s first Bill Committee, but the job of the Opposition is to test the definitions in the Bill and ensure that it is fit for purpose. My concern is that the definition of high risk is set too high to cover law enforcement agencies and will allow egregious breaches of individuals’ data rights, privacy rights and right to liberty. It is our job as the Opposition—there is nothing wrong with us exercising this role—to ensure that the Bill is fit for purpose. That is what we are seeking to do.

Victoria Atkins: I am extremely grateful to the hon. Lady for clarifying her role. My answer is exactly as I said before. High risk includes processing where there is a particular likelihood of prejudice to the rights and freedoms of data subjects. That must be a matter for the data controller to assess. We cannot assess it here in Committee for the very good reason put forward by members of the Committee: we cannot foresee every eventuality. Time will move on, as will technology. That is why the Bill is worded as it is, to try to future-proof it but also, importantly, because the wording complies with our obligations under the law enforcement directive and under the modernised draft Council of Europe convention 108.

Liam Byrne: Does the Minister not have some sympathy with the poor individuals who end up being data controllers for our police forces around the country, given the extraordinary task that they have to do? She is asking those individuals to come up with their own frameworks of internal guidance for what is high, medium and low risk. The bureaucracy-manufacturing potential of the process she is proposing will be difficult for police forces. We are trying to help the police to do their job, and she is not making it much easier.
Victoria Atkins: Clause 65(2) states:

“The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section 64 indicates that the processing of the data would result in a high risk.”

There are many complicated cases that the police and others have to deal with. That is why we have guidance rather than putting it in statute—precisely to give those on the frontline the flexibility of understanding. “This situation has arisen, and we need to calibrate the meaning of high risk and take that into account when we look at the prejudices caused to a person or a group of people.” That is precisely what we are trying to encompass. Presumably, that is what the Council of Europe and those involved in drafting the law enforcement directive thought as well.

Of course, there will be guidance from the Information Commissioner to help data controllers on those assessments, to enable us to get a consistent approach across the country. That guidance will be the place to address these concerns, not on the face of the Bill.

Louise Haigh: Can the Minister confirm that the Metropolitan police consulted the Information Commissioner before trialling facial recognition software? I appreciate that she might not be able to do so on her feet, so I will of course accept it if she wishes to write to me.

Victoria Atkins: I am afraid that I will have to write to the hon. Lady on that.

The intention behind this part of the Bill is not to place unnecessary barriers in the way of legitimate processing. Nor, we all agree, should we place additional burdens on the commissioner without there being a clear benefit. These provisions are in the Bill to address the need for an intelligent application of the data protection safeguards, rather than assuming that a one-size-fits-all approach results in better data protection.

Amendment 149 would insert a new subsection (8) to clause 65, which would permit the commissioner to exercise powers of enforcement if she was not satisfied that the controller or processor had taken sufficient steps to act on her opinion that intended processing would infringe the provisions in part 3. It is worth noting that the purpose of clause 65 is to ensure consultation with the commissioner prior to processing taking place. It is therefore not clear what enforcement the commissioner would be expected to undertake in this instance, as the processing would not have taken place. If, however, the controller sought to process the data contrary to the commissioner’s opinion, it would be open to her to take enforcement action in line with her powers already outlined in part 6.

I do not know, Mr Hanson, whether we have dealt with new clauses 3 and 4.

The Chair: New clauses 3 and 4 are being considered as part of this group, but would not be voted on until after the consideration of the clauses of the Bill have been completed. If you wish to respond to them, Minister, you can do so now.

Victoria Atkins: I am grateful; I will deal with them now. New clauses 3 and 4 would place additional obligations on the intelligence services. New clause 3 would require the intelligence services to undertake a data protection impact assessment in cases where there is a risk to the rights and freedoms of individuals, whereas new clause 4 would require the intelligence services to have prior consultation with the Information Commissioner when proposing processing. Neither new clause reflects the unique form of processing undertaken by the intelligence services, its sensitive nature and the safeguards that already exist.

I should stress that the “data protection by design” requirements of clause 103 are wholly consistent with draft modernised Council of Europe convention 108, which was designed to apply to the processing of personal data in the national security context, and which therefore imposes proportionate requirements and safeguards. Under clause 103, in advance of proposing particular types of processing, the intelligence services will be obliged to consider the impact of such processing on the rights and freedoms of data subjects. That requirement will be integrated into the design and approval stages of the delivery of IT systems that process personal data, which is the most effective and appropriate way to address the broad aim. Furthermore, clause 102 requires the controller to be able to demonstrate, particularly to the Information Commissioner, that the requirements of chapter 4 of part 4 of the Bill are complied with, including the requirement in clause 103 to consider the impact of processing.

4 pm

The impact assessment requirements of the general data protection regulation and the law enforcement directive were not designed for national security processing, which is out of the scope of EU law. Given the need to respond swiftly and decisively in the event of terrorist acts or actions by hostile states, any unnecessary delay to the intelligence services’ ability to deal with such threats could clearly have serious consequences. The new clauses are therefore inappropriate and could prejudice the lawful and proportionate action that is required to safeguard UK national security and UK citizens. Having explained our reasoning behind clauses 64 and 65, I hope that the hon. Member for Sheffield, Heeley will withdraw her amendment.

Louise Haigh: I remain concerned that the Bill leaves gaps that will enable law enforcement agencies and the police to go ahead and use technology that has not been tested and has no legal basis. As my right hon. Friend the Member for Birmingham, Hodge Hill said, that leaves the police open to having to develop their own guidance at force level, with all the inconsistencies that would entail across England and Wales.

The Minister agreed to write to me on a couple of issues. I do not believe that the Metropolitan police consulted the Information Commissioner before trialling the use of photo recognition software, and I do not believe that other police forces consulted the Information Commissioner before rolling out mobile fingerprint scanning. If that is the case and the legislation continues with the existing arrangements, that is not sufficient. I hope that before Report the Minister and I can correspond so as potentially to strengthen the measures. With that in mind, and with that agreement from the Minister, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.
Clause 67

**Notification of a personal data breach to the Commissioner**

**Question proposed, That the clause stand part of the Bill.**

**Liam Byrne:** The Committee is looking for some guidance and for tons of reassurance from the Minister about how the clause will bite on data processors who do not happen to base their operations here in the United Kingdom. This morning we debated the several hundred well-known data breaches around the world and highlighted some of the more recent examples, such as Yahoo!—that was probably the biggest—and AOL. More recently, organisations such as Uber have operated their systems with such inadequacy that huge data leaks have occurred, directly infringing the data protection rights of citizens in this country. The Minister will correct me if I am wrong, but I am unaware of any compensation arrangements that Uber has made with its drivers in this country whose data was leaked.

Even one of the companies closest to the Government—Equifax, which signed a joint venture agreement with the Government not too long ago—has had a huge data breach. It took at least two goes to get a full account from Equifax of exactly what had happened, despite the fact that Her Majesty’s Government was its corporate partner and had employed it through the Department for Work and Pensions. All sorts of information sharing happened that never really came to light. I am not sure whether any compensation for Equifax data breaches has been paid to British citizens either.

My point is that most citizens of this country have a large amount of data banked with companies that operate from America under the protection of the first amendment. There is a growing risk that in the years to come, more of the data and information service providers based in the UK will go somewhere safer, such as Ireland, because they are worried about the future of our adequacy agreement with the European Commission. We really need to understand in detail how the Information Commissioner, who is based here, will take action on behalf of British citizens against companies in the event of data breaches. For example, how will she ensure notification within 72 hours? How will she ensure the enforcement of clause 67(4), which sets out the information that customers and citizens must be told about the problem?

This morning we debated the Government’s ludicrous proposals for class action regimes, which are hopelessly inadequate and will not work in practice. We will not have many strong players in the UK who are able to take action in the courts, so we will be wholly reliant on the Information Commissioner to take action. I would therefore be grateful if the Minister reassured the Committee how the commissioner will ensure that clause 67 is enforced if the processor of the data is not on our shores.

**Victoria Atkins:** The right hon. Gentleman refers to companies not on these shores, about which we had a good deal of discussion this morning. Clause 67 belongs to part 3 of the Bill, which is entitled “Law enforcement processing”, so I am not sure that the companies that he gives as examples would necessarily be considered under it. I suppose a part 3 controller could have a processor overseas, but that would be governed by clause 59. Enforcement action would, of course, be taken by the controller under part 3, but I am not sure that the right hon. Gentleman’s examples are relevant to clause 67.

**Liam Byrne:** I am grateful to the Minister for that helpful clarification. Let me phrase the question differently, with different examples. The Home Office and many police forces are outsourcing many of their activities, some of which are bound to involve data collected by global organisations such as G4S. Is she reassuring us that any and all data collected and processed for law enforcement activities will be held within the boundaries of the United Kingdom and therefore subject to easy implementation of clause 67?

**Victoria Atkins:** The controller will be a law enforcement agency, to which part 3 will apply. I note that clause 200 provides details of the Bill’s territorial application should a processor be located overseas, but under part 3 it will be law enforcement agencies that are involved.

**Liam Byrne:** Where G4S, for example, is employed to help with deportations, the Minister is therefore reassuring us that the data controller would never be G4S. However, if there were an activity that was clearly a law enforcement activity, such as voluntary removal, would the data controller always be in Britain and therefore subject to clause 67, even where private sector partners are involved? The Minister may outsource the contract, but we want to ensure that she does not outsource the role of data controller so that a law enforcement activity here can have a data controller abroad.

**Victoria Atkins:** I appreciate the sentiment behind the amendment. If the Home Office outsources processing to an overseas company, any enforcement action would be taken against the Home Office as the controller. The right hon. Gentleman has raised the example of G4S in the immigration context, so I will reflect on that overnight and write to him to ensure that the answer I have provided also covers that situation.

**Question put and agreed to.**

Clause 67 accordingly ordered to stand part of the Bill.

Clause 68 to 71 ordered to stand part of the Bill.

Clause 72

**Overview and interpretation**

**Question proposed, That the clause stand part of the Bill.**

**Liam Byrne:** I want to flag up an issue that we will stumble across in a couple of stand part debates: the safeguards that will be necessary for data sharing between this country and elsewhere. We will come on to the safeguards that will be necessary for the transfer of data between our intelligence agencies and foreign intelligence agencies. Within the context of this clause, which touches on the broad principle of data sharing from here and abroad, I want to rehearse one or two arguments on which Ministers should be well briefed and alert.
Our intelligence agencies do an extraordinary job in keeping this country safe, which sometimes involves the acquisition and use of data that results in the loss of life. All Committee members will be familiar with the drone strike that killed Reyaad Khan and Ruhul Amin, and many of us will have heard the Prime Minister’s assurances in the Liaison Committee about the robust legal process that was gone through to ensure that the strike was both proportionate and legal.

The challenge—the public policy issue that arises under chapter 5 of the Bill—is that there is a number of new risks. First, there is the legal risk flagged up by the Court of Appeal in 2013, when justices said that it was not clear that UK personnel will be immune from criminal liability for their involvement in a programme that involves the transfer of intelligence from an intelligence service here to an American partner and where that American partner uses that information to conduct drone strikes that involve the loss of life. Confidence levels differ, but we in the Committee are pretty confident about the legal safeguards around those kinds of operations in this country. We can be less sure about the safeguards that some of our partners around the world have in place. The Court of Appeal has expressed its view, which was reinforced in 2016 by the Joint Committee on Human Rights. The Committee echoed the finding that “front-line personnel…should be entitled to more legal certainty” than they have today.

This section of the Bill gives us the opportunity to ensure that our intelligence services are equipped with a much more robust framework than they have today, to ensure that they are not subject to the risks flagged by the Court of Appeal or by the Joint Committee on Human Rights.

4.15 pm

We have shared intelligence with our partners, particularly in the Five Eyes network, for many moons. We have great specialism in that area. We have a number of RAF bases in this country and abroad with particularly important capabilities, and our facility in Cheltenham is pretty much the best in the world. We have to confront the challenge that the governance of some of our Five Eyes partners is perhaps not as cautious as the leadership of those countries was in the past. Since the election of President Trump, there has been a dramatic increase in the United States’ drone programme.

We need to face up to the challenge—not duck, ignore, or pretend it is not there—that we want to preserve the legal safeguards that ensure that our intelligence services can do their job. We want to ensure that there are good, strong, robust arrangements for sharing intelligence with our partners.

We do not want to jeopardise our intelligence services or the information sharing agreements because of the misuse of intelligence by our partners abroad. That is particularly important when our partners abroad are deploying legal force in countries such as Syria, northern Iraq and, increasingly, Yemen, where the number of drone strikes has increased by 288% in recent years.

On this clause, it is appropriate to say that we want to have a good debate about what the safeguards need to look like to ensure good and safe intelligence sharing between our agencies. We hope the Government will be open-minded and will acknowledge our objective. The life of our intelligence services is complicated enough without having to question whether what they are doing is legally viable and whether it will be subject to legal challenge in the future. I hope we can reflect on that correctly, because we are not entirely sure that the safeguards in the Bill are robust enough.

Victoria Atkins: We are still on part 3, which deals with law enforcement processing. It does not relate to processing by security services. We will come to that when we debate amendment 159 to clause 109, so I reserve the right to respond to those observations on that amendment in due course.

The Chair: There is no amendment before the Committee. We are on clause 72. The right hon. Member for Birmingham, Hodge Hill made some comments, which I did not rule out of order. The Minister has indicated that she will respond to the wider issue of concerns about drones and national security at a later date. That is a matter for her. If the right hon. Gentleman is happy with that, and if the Minister is content, I will put the question that the clause stand part of the Bill.

Question put and agreed to.

Clause 72 accordingly ordered to stand part of the Bill. Clauses 73 to 86 ordered to stand part of the Bill.

Ordered. That further consideration be now adjourned.—(Nigel Adams.)

4.21 pm

Adjourned till Tuesday 20 March at twenty-five minutes past Nine o’clock.
Written evidence reported to the House
DPB 25 Open Rights Group and the3million
DPB 26 defenddigitalme
DPB 27 Reprieve
DPB 28 Association of British Insurers (ABI)
DPB 29 Associated Newspapers
DPB 30 European Justice Forum

DPB 31 Press Recognition Panel
DPB 32 Which?
DPB 33 Open Rights Group and Chris Pounder
DPB 34 Baylis Media Ltd
DPB 35 Personal Investment Management & Financial Advice Association (PIMFA)
DPB 36 Robin Makin
DPB 37 Robin Makin (Chapter 3 of Part 4)
CONTENTS

Schedules 9 and 10 agreed to, one with an amendment.
Clauses 87 to 112, some with amendments.
Schedule 11 agreed to, with amendments.
Clauses 113 and 114 agreed to.
Schedule 12 agreed to.
Clauses 115 and 116 agreed to.
Schedule 13 agreed to, with an amendment.
Clauses 117 and 118 agreed to.
Schedule 14 agreed to.
Clauses 119 and 120 agreed to.
Clause 121 disagreed to.
Clauses 122 to 131 agreed to, some with an amendment.
Adjourned till this day at Two o’clock.
No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Saturday 24 March 2018
The Committee consisted of the following Members:

**Chairs:** †David Hanson, Mr Gary Streeter

† Adams, Nigel *(Lord Commissioner of Her Majesty’s Treasury)*
† Atkins, Victoria *(Parliamentary Under-Secretary of State for the Home Department)*
† Byrne, Liam *(Birmingham, Hodge Hill) (Lab)*
† Clark, Colin *(Gordon) (Con)*
† Elmore, Chris *(Ogmore) (Lab)*
† Haigh, Louise *(Sheffield, Heeley) (Lab)*
† Heaton-Jones, Peter *(North Devon) (Con)*
† Huddleston, Nigel *(Mid Worcestershire) (Con)*
† Jack, Mr Alister *(Dumfries and Galloway) (Con)*
† James, Margot *(Minister of State, Department for Digital, Culture, Media and Sport)*
† Jones, Darren *(Bristol North West) (Lab)*
† Lopez, Julia *(Hornchurch and Upminster) (Con)*
† McDonald, Stuart C. *(Cumbernauld, Kilsyth and Kirkintilloch East) (SNP)*
† Murray, Ian *(Edinburgh South) (Lab)*
† O’Hara, Brendan *(Argyll and Bute) (SNP)*
† Snell, Gareth *(Stoke-on-Trent Central) (Lab/Co-op)*
† Warman, Matt *(Boston and Skegness) (Con)*
† Wood, Mike *(Dudley South) (Con)*
† Zeichner, Daniel *(Cambridge) (Lab)*

Kenneth Fox, Committee Clerk

† attended the Committee
Public Bill Committee

Tuesday 20 March 2018

(Morning)

[David Hanson in the Chair]

Data Protection Bill [Lords]

9.25 am

The Chair: We begin consideration of the Bill today with schedule 9, to which no amendments have been tabled.

Schedule 9 agreed to.

Schedule 10

Conditions for sensitive processing under Part 4

Amendment made: 117, in schedule 10, page 187, line 5, at end—

‘Safeguarding of children and of individuals at risk

3A (1) This condition is met if—

(a) the processing is for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is “at risk” if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.”—(Victoria Atkins.)

Schedule 10 makes provision about the circumstances in which the processing of special categories of personal data is permitted. This amendment adds to that Schedule certain processing of personal data which is necessary for the protection of children or of adults at risk. See also Amendments 85 and 116.

Schedule 10, as amended, agreed to.

Clauses 87 to 93 ordered to stand part of the Bill.

Clause 94

Right of access

Amendments made: 35, in clause 94, page 55, line 9, leave out ‘day’ and insert ‘time’

This amendment is consequential on Amendment 71.

36, in clause 94, page 55, line 9, leave out ‘day’ and insert ‘time’

This amendment is consequential on Amendment 71.

37, in clause 94, page 55, line 10, leave out ‘days’

This amendment is consequential on Amendment 71.

38, in clause 94, page 55, line 11, leave out ‘the day on which’ and insert ‘when’

This amendment is consequential on Amendment 71.

39, in clause 94, page 55, line 12, leave out ‘the day on which’ and insert ‘when’

This amendment is consequential on Amendment 71.

40, in clause 94, page 55, line 13, leave out ‘the day on which’ and insert ‘when’—(Victoria Atkins.)

This amendment is consequential on Amendment 71.

Clause 94, as amended, ordered to stand part of the Bill.

Clause 96

Right not to be subject to automated decision-making

Question proposed, That the clause stand part of the Bill.

Liam Byrne (Birmingham, Hodge Hill) (Lab): We are rattling through the Bill this morning and will soon reach clause 109, to which we have tabled some amendments. Clause 96, within chapter 3 of part 4, on intelligence services processing, touches on the right not to be subject to automated decision making. I do not want to rehearse the debate that we shall have later, but I think that this is the appropriate point for an explanation from the Minister. Perhaps she will say something about the kind of administration that the clause covers, and its relationship, if any—there may not be one, but it is important to test that question—to automated data-gathering by our intelligence services abroad, and the processing and use of that data.

The specific instance that I want to take up concerns the fact that about 700 British citizens have gone to fight in foreign conflicts—for ISIS in particular. The battery of intelligence-gathering facilities that we have allows us to use remote data-sensing to detect, track and monitor them, and to assemble pictures of their patterns of life and behaviour. It is then possible for our intelligence services to do stuff with those data and patterns, such as transfer them to the military or to foreign militaries in coalitions of which we are a member. For the benefit of the Committee, will the Minister spell out whether the clause, and potentially clause 97, will bite on that kind of capability? If not, where are they aimed?

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): An intelligence services example under clause 96 would be a case where the intelligence services wanted to identify a subject of
interest who might have travelled to Syria in a certain time window and where the initial selector was age, because there was reliable reporting that the person being sought was a certain age. The application of the age selector would produce a pool of results, and a decision may be taken to select that pool for further processing operations, including the application of other selectors. That processing would be the result of a decision taken solely on the basis of automated processing.

Liam Byrne: I do not think the clause actually says anything about age selection. How do we set boundaries around the clause? Let us say that minors—people under the age of 18—want to travel to Syria or some other war zone. Is the Minister basically saying that the clause will bite on that kind of information and lead to a decision chain that results in action to intervene? If that is the case, will she say a little more about the boundaries around the use of the clause?

Victoria Atkins: The right hon. Gentleman asked me for an example and I provided one. Age is not in the clause because the Government do not seek in any way to create burdens for the security services when they are trying to use data to protect this country. Given his considerable experience in the Home Office, he knows that it would be very peculiar, frankly, for age to be listed specifically in the clause. The clause is drafted as it is, and I remind him that it complies with Council of Europe convention 108, which is an international agreement.

Liam Byrne: The point is that the clause does create a burden. It does not detract from a burden; it creates an obligation on intelligence services to ensure that there is not automatic decision making. We seek not to add burdens, but to question why the Minister is creating them.

Victoria Atkins: The clause complies with Council of Europe convention 108. I do not know whether I can say any more.

The Chair: I think we have come to a natural conclusion.

Question put and agreed to.

Clause 96 accordingly ordered to stand part of the Bill.

Clause 97

RIGHT TO INTERVENE IN AUTOMATED DECISION-MAKING

Amendments made: 41, in clause 97, page 56, line 34, leave out “21 days” and insert “1 month”.

Clause 97(4) provides that where a controller notifies a data subject under Clause 97(1) that the controller has taken a decision falling under Clause 97(1) (automated decisions required or authorised by law), the data subject has 21 days to request the controller to reconsider or take a new decision not based solely on automated processing. This amendment extends that period to one month.

Amendment 42, in clause 97, page 56, line 39, leave out “21 days” and insert “1 month”.—(Victoria Atkins.)

Clause 97(5) provides that where a data subject makes a request to a controller under Clause 97(4) to reconsider or retake a decision based solely on automated processing, the controller has 21 days to respond. This amendment extends that period to one month.

Clause 97, as amended, ordered to stand part of the Bill.

Clause 98

RIGHT TO INFORMATION ABOUT DECISION-MAKING

Question proposed, That the clause stand part of the Bill.

Liam Byrne: This is a vexed and difficult area. The subject of the clause is the right to information about decision making, which is very difficult when it comes to the intelligence services, and I have had experiences, as have others I am sure, of constituents who come along to an advice bureau and claim to have been subject either to intelligence services investigation or, in some cases, to intelligence services trying to recruit them. Sometimes—this is not unknown—an individual’s immigration status might be suspect. I had one of these cases about five or six years ago, where the allegation was that the intelligence services were conspiring with the UK Border Agency and what at that time was the Identity and Passport Service to withhold immigration documents to encourage the individual to become a source. The challenge for Members of Parliament trying to represent such individuals is that they will get a one-line response when they write to the relevant officials to say, “I am seeking to represent my constituent on this point.”

A right to information about decision-making will be created under clause 98. I ask the Minister, therefore, when dealing with very sensitive information, how is this right going to be exercised and who is going to be the judge of whether that right has been fulfilled satisfactorily? There is no point approving legislation that is superfluous because it will have no effect in the real world. The clause creates what looks like a powerful new right for individuals to request information about decisions taken by the intelligence agencies, which might have a bearing on all sorts of things in their lives. Will the Minister explain how, in practice, this right is to become a reality?

Victoria Atkins: If I may give an example, where a terrorist suspect is arrested and believes he is the subject of MI5 surveillance, revealing to them whether they were under surveillance and the process by which the suspect was identified as a potential terrorist would clearly aid other terrorists in avoiding detection. The exercise of the right is subject to the operation of the national security exemption, which was debated at length last week. It might be that, in an individual case, the intelligence services need to operate the “neither confirm nor deny” principle, and that is why the clause is drafted as it is.

Liam Byrne: The clause is drafted in the opposite way. Subsection (1)(b) says that “the data subject is entitled to obtain from the controller, on request, knowledge of the reasoning underlying the processing.” In other words, the data subject—in this case, the individual under surveillance—has the right to obtain from the controller, in the hon. Lady’s example of the intelligence agencies, knowledge of the reasoning underlying the way their data was processed.

Let us take, for example, a situation where CCTV footage was being captured at an airport or a border crossing and that footage was being run through facial
[Liam Byrne]

recognition software, enabling special branch officers to intervene and intercept that individual before they crossed the border. That is an example of where information is captured and processed, and action then results in an individual, in this case, being prevented from coming into the country.

I have often had cases of constituents who have come back from Pakistan or who might have transitioned through the middle east, perhaps Dubai, and they have been stopped at Birmingham airport because special branch officers have said their name is on a watch list. Watch lists are imperfect—that is probably a fairly good description. They are not necessarily based on the most reliable and up-to-date information, but advances in technology allow a much broader and more wide-ranging kind of interception to take place at the border. If we are relying not on swiping someone’s passport and getting a red flag on a watch list but on processing data coming in through CCTV and running it through facial recognition software, that is a powerful new tool in the hands of the intelligence agencies. Subsection (1)(b) will give one of my constituents the right to file a request with the data controller—presumably, the security services—and say, “Look, I think your records are wrong here. You have stopped me on the basis of facial recognition software at Birmingham airport; I want to know the reasoning behind the processing of the data.”

If, as the Minister says, the response from the data controller is, “We can neither confirm nor deny what happened in this case,” then, frankly, the clause is pretty nugatory. Will the Minister give an example of how the right is going to be made a reality? What are the scenarios in which a constituent might be able to exercise this right? I am not interested in the conventions and so on, but I am afraid we are conferring on the data subject are too sweeping. We might be concerned that there are insufficient safeguards in place for the intelligence agencies to do their jobs. This is a specific question about how data subjects, under the clause, are going to exercise their power in a way that allows the security services to do their job. That is not a complicated request; it is a basic question.

Victoria Atkins: As I say, the framework is set out in the Bill, and the exemption exists in the Bill itself. I have already given an example about a terror suspect. With respect, I am not going to enter into this debate about the right hon. Gentleman’s constituent—what he or she might have requested, and so on. The framework is there; the right is there, balanced with the national security exemption. I am not sure there is much more I can add.

Liam Byrne: The Minister says she does not want to enter into a debate. I kindly remind her that she in a debate. The debate is called—

Victoria Atkins: Mr Hanson, I did not say that.

The Chair: Order. Liam Byrne has the floor. If he wishes to give way, he may do so.

Victoria Atkins: On a point of order, Mr Hanson. I did not say that I do not want a debate. Will the right hon. Gentleman please use his language carefully, as I know he has long experience of doing? I said I was not sure how fruitful it would be to have examples, to and fro, about constituents. That is quite a different matter from a debate. I have debated with him; I have said the answer; it is for him—

9.45 am

The Chair: Order. We have a point of order—which, in due course, the good offices of Hansard will resolve—as to what was said by the right hon. Gentleman and how the Minister interpreted it. At the moment, we are dealing with clause 98 and Mr Liam Byrne has the floor. As he wishes, he can give way or continue.

Liam Byrne: I am grateful, Mr Hanson, for that complete clarity. This is the debate that we are having today: how will clause 98(1)(b) become a reality? It creates quite powerful rights for a data subject to seek information from the intelligence agencies. I gave an example from my constituency experience of how the exercise of this right could run into problems.

All I ask of the Minister responsible for the Bill and this area of policy, who has thought through the Bill with her officials and is asking the Committee to agree
the power she is seeking to confer on our constituents, and who will have to operate the policy in the real world after the Bill receives Royal Assent, is that she gives us a scenario of how the rights she is conferring on a data subject will function in the real world.

However, Mr Hanson, I think we might have exhausted this debate. It is disappointing that the Minister has not been able to come up with a scenario. Perhaps she would like to intervene now to give me an example.

**Victoria Atkins:** Part 4 sets out a number of rights of data subjects, clause 98 being just one of them. This part of the Bill reflects the provisions of draft modernised convention 108, which is an international agreement, and the Bill faithfully gives effect to those provisions. A data subject wishing to exercise the right under clause 98 may write to that effect to the Security Service, which will then either respond in accordance with clause 98 or exercise the national security exemption in clause 110. That is the framework.

**Liam Byrne:** That is probably as much reassurance as the Committee is going to get this afternoon. It is not especially satisfactory or illuminating, but we will not stand in the way and we will leave the debate there, Mr Hanson.

**The Chair:** This might seem like a long day, but it is still morning. On that note, we will proceed.

**Question put and agreed to.**

Clause 98 accordingly ordered to stand part of the Bill.

**Clause 99**

**RIGHT TO OBJECT TO PROCESSING**

*Amendments made:* 43, in clause 99, page 57, line 28, leave out “day” and insert “time”.

*This amendment is consequential on Amendment 71.*

44, in clause 99, page 58, line 3, leave out “day” and insert “time”.

*This amendment is consequential on Amendment 71.*

45, in clause 99, page 58, line 5, leave out “the day on which” and insert “when”.

*This amendment is consequential on Amendment 71.*

46, in clause 99, page 58, line 6, leave out “the day on which” and insert “when” — (Victoria Atkins.)

*This amendment is consequential on Amendment 71.*

Clause 99, as amended, ordered to stand part of the Bill.

Clauses 100 to 108 ordered to stand part of the Bill.

**Clause 109**

**TRANSFERS OF PERSONAL DATA OUTSIDE THE UNITED KINGDOM**

**Liam Byrne:** I beg to move amendment 159, in clause 109, page 61, line 13, after “is” insert “provided by law and is”.

*This amendment would place meaningful safeguards on the sharing of data by the intelligence agencies.*

The Chair: With this it will be convenient to discuss the following:

Amendment 160, in clause 109, page 61, line 18, at end insert—

‘(3) The transfer falls within this subsection if the transfer—

(a) is based on an adequacy decision (see section 74),

(b) if not based on an adequacy decision, is based on there being appropriate safeguards (see section 75), or

(c) if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances (see section 76 as amended by subsection (5)).

(4) A transfer falls within this subsection if—

(a) the intended recipient is a person based in a third country that has (in that country) functions comparable to those of the controller or an international organisation, and

(b) the transfer meets the following conditions—

(i) the transfer is strictly necessary in a specific case for the performance of a task of the transferring controller as provided by law or for the purposes set out in subsection (2),

(ii) the transferring controller has determined that there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer,

(iii) the transferring controller informs the intended recipient of the specific purpose or purposes for which the personal data may, so far as necessary, be processed, and

(iv) the transferring controller documents any transfer and informs the Commissioner about the transfer on request.

(5) The reference to law enforcement purposes in subsection (4) of section 76 is to be read as a reference to the purposes set out in subsection (2).’

New clause 14—Subsequent transfers—

‘(1) Where personal data is transferred in accordance with section 109, the transferring controller must make it a condition of the transfer that the data is not to be further transferred to a third country or international organisation without the authorisation of the transferring controller.

(2) A transferring controller may give an authorisation under subsection (1) only where the further transfer is necessary for the purposes in subsection (2).

(3) In deciding whether to give the authorisation, the transferring controller must take into account (among any other relevant factors)—

(a) the seriousness of the circumstances leading to the request for authorisation,

(b) the purpose for which the personal data was originally transferred, and

(c) the standards for the protection of personal data that apply in the third country or international organisation to which the personal data would be transferred.’

*This new clause would place meaningful safeguards on the sharing of data by the intelligence agencies.*

**Liam Byrne:** I rise to speak to amendments 159 and 160, which relate to two significant developments in defence policy that have unfolded over the past couple of years. Our intelligence agencies have acquired pretty substantial new capabilities through all kinds of technological advances, which allow them remotely to collect and process data in a completely new way.
It is now possible, through satellite technology and drones, to collect video footage of battle zones and run the information collected through facial recognition software, which allows us to track much more forensically and accurately the movement, habits, working lives and leisure of bad people in bad places. We are fighting against organisations such as Daesh, in a coalition with allies, but over the past year one of our allies has rather changed the rules of engagement, which allows it to take drone strikes with a different kind of flexibility from that under the Obama regime.

The change in the American rules of engagement means that, on the one hand, the American Administration has dramatically increased the number of drone strikes—in Yemen, we have had an increase of about 288% in the past year—and, on the other, as we see in other theatres of conflict such as the war against al-Shabaab in Africa, repeated strikes are allowed for. Therefore, even when the circumstances around particular individuals have changed—new intelligence may have come to light about them—the Trump Administration have basically removed the safeguards that President Obama had in place that require an individual to be a “continuing and imminent threat” before a strike is authorised. That safeguard has been lifted, so the target pool that American forces can take aim at and engage is now much larger, and operational commanders have a great deal more flexibility over when they can strike.

We now see some of the consequences of that policy, with the most alarming statistics being on the number of civilians caught up in some of those strikes. That is true in Yemen and in the fight against al-Shabaab, and I suspect it is true in Syria, Afghanistan and, in some cases, Pakistan. We must ensure that the data sharing regime under which our intelligence agencies operate does not create a legal threat to them because of the way the rules of engagement of one of our allies have changed.

The Joint Committee on Human Rights has talked about that, and it has been the subject of debates elsewhere in Parliament. The JCHR concluded in its 2016 report that

“we owe it to all those involved in the chain of command for such uses of lethal force—intelligence personnel, armed services personnel, officials, Ministers and others—to provide them with absolute clarity about the circumstances in which they will have a defence against any possible future criminal prosecution, including those which might originate from outside the UK.”

We need to reflect on some of those legal risks to individuals who are serving their country. The amendment would ensure that—where there was a collection, processing and transfer of information by the UK intelligence services to one of our allies, principally America, and they ran that information against what is widely reported as a kill list and ordered drone strikes without some of the safeguards operated by previous Administrations—first, the decision taken by the intelligence agency here to share that information was legal and, secondly, it would be undertaken in a way that ensured that our serving personnel were not subject to legal threats or concerns about legal threats.

Mike Wood (Dudley South) (Con): Does the right hon. Gentleman agree that the legal framework that we rightly expect to apply to our law enforcement offers and agencies does not necessarily apply directly to our intelligence and security services? That, however, would be the effect of the amendment.

Liam Byrne: I am not sure that that would be the effect of the amendment. While I agree with the thrust of the hon. Gentleman’s argument, I am cognisant of the fact that in 2013 the Court of the Appeal said that it was “certainly not clear” that UK personnel would be immune from criminal liability for their involvement in a programme that entailed the transfer of information to America and a drone strike ordered using that information, without the same kinds of safeguard that the Obama Administration had. The amendment would ensure a measure—nothing stronger than that—of judicial oversight where such decisions were taken and where information was transferred. We must ensure a level of judicial oversight so that inappropriate decisions are not taken. It is sad that we need such a measure, but it reflects two significant changes over the past year or two: first, the dramatic increase in our ability to capture and process information; and, secondly, the crucial change in the rules of engagement under the Trump Administration.

Mike Wood: The right hon. Gentleman is being kind and generous with his time. He says that the amendments would not replicate the frameworks for law enforcement, yet amendment 160 would do exactly that by applying clauses 74, 75 and 76 to the test for data sharing for intelligence and security services. Those exact safeguards were designed for law enforcement, not for intelligence and security sharing.

Liam Byrne: The point for the Committee is that the thrust of the amendment is not unreasonable. Where there is a multiplication of the power of intelligence agencies to capture and process data, it is not unreasonable to ask for that greater power to bring with it greater scrutiny and safeguards. The case for this sensible and cautious amendment is sharpened because of the change in the rules of engagement operated by the United States. No member of the Committee wants a situation where information is transferred to an ally, and that ally takes a decision that dramatically affects the human rights of an individual—as in, it ends those rights by killing that person. That is not something that we necessarily want to facilitate.

As has been said, we are conscious of the difficulty and care with which our politicians have sometimes had to take such decisions. The former Prime Minister very sensibly came to the House to speak about his decision to authorise a drone strike to kill two British citizens whom he said were actively engaged in conspiring to commit mass murder in the United Kingdom. His judgment was that those individuals posed an imminent threat, but because they were not operating in a place where the rule of law was operational, there was no possibility to send in the cops, arrest them and bring them to trial.

The Prime Minister was therefore out of options, but the care that he took when taking that decision and the level of legal advice that he relied on were extremely high. I do not think any member of the Committee is confident that the care taken by David Cameron when he made that decision is replicated in President Trump’s White House.
We must genuinely be concerned and cautious about our intelligence agencies transferring information that is then misused and results in drone strikes that kill individuals, without the safeguards we would expect. The last thing anyone would want is a blowback, in either an American or a British court, on serving officers in our military or intelligence services because the requisite safeguards simply were not in place.

My appeal to the Committee is that this is a point of principle: enhanced power should bring with it enhanced oversight and surveillance, and the priority for that is the fact that the rules of engagement for the United States have changed. If there is a wiser way in which we can create the kinds of safeguard included in the amendment we will all ears, but we in the House of Commons cannot allow the situation to go unchecked. It is too dangerous and too risky, and it poses too fundamental a challenge to the human rights that this place was set up to champion and protect.

10 am

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): I agree that these amendments ask a legitimate and important question about the level of safeguards on international data sharing by UK intelligence agencies. As it stands, clause 109 contains two fairly otiose sub- clauses to do with the sharing of personal data abroad by our intelligence agencies. In contrast, there is a whole chapter and a full seven clauses putting in place safeguards in relation to transfer to third countries by law enforcement agencies. These amendments borrow some of the safeguards placed on law enforcement agencies and there seems to be no good reason why that is not appropriate. I take the point that it does not necessarily follow that what is good for law enforcement agencies is definitely good for intelligence services. However, it is for the Government to tell us why those safeguards are not appropriate. If there are different ways for us to go about this, I am all ears, like the right hon. Gentleman. The right hon. Gentleman quite rightly raised the example of drones and US attacks based on information shared by personnel. At the moment, the lack of safeguards and of a very clear legal basis for the transfer of information can be lethal for billions and is dangerous for our personnel, as the Joint Committee on Human Rights has pointed out.

We support the thrust of these amendments.

Darren Jones (Bristol North West) (Lab): I declare my interests as set out in the Register of Members’ Interests.

The Chair: Order. The hon. Gentleman declared his interests in previous Committees, but I have been advised that he needs to specify what the interests are, as well as declaring them.

Darren Jones: Thank you, Mr Hanson. The two items on the register are, first, that I was a legal counsel at BT before my election as a Member of Parliament, where I was responsible for data protection law. Secondly, I had a relationship with a law firm called Kemp Little to maintain my practising certificate while I was a Member of Parliament.

My argument in support of amendment 160 is one that I have rehearsed in previous debates. In line with recommendations from the Joint Committee on Human Rights, today we benefit from an exemption under European treaties that say that national security is a member state competence and therefore not one with which the European Union can interfere. However, if the UK leaves the European Union, the European Commission reserves the right to review the entire data processing legislation, including that for intelligence services of a third country when seeking to make a decision on adequacy—as it has done with Canada. Where the amendment talks about adequacy, it would be helpful—

Victoria Atkins: Does the EU have an adequacy agreement with Canada?

Darren Jones: It does, but it has been reviewed by the European Commission. One of the concerns the Commission has had with Canada is its intelligence-sharing arrangements with the United States of America, which is why this amendment is so pertinent and why it is right to support the Government in seeking this adequacy decision. I make the point again that we will no longer benefit from the exemption if we leave the European Union and I hope that the Government keep that in mind.

Victoria Atkins: Before I start, I want to clarify what the hon. Gentleman has just said about adequacy decisions. Canada does have an adequacy decision from the EU for transfers to commercial organisations that are subject to the Canadian Personal Information Protection and Electronic Documents Act. I am not sure that security services are covered in that adequacy decision, but it may be that we will get assistance elsewhere.

As the right hon. Member for Birmingham, Hodge Hill is aware, amendments 159, 160 and new clause 14 were proposed by a campaigning organisation called Reprieve in its recent briefing on the Bill. They relate to concerns about the sharing of personal data with the US and seek to apply the data sharing protections designed specifically for law enforcement data processing, provided for in part 3 of the Bill, to processing by the intelligence services, provided for in part 4. That is, they are seeking to transpose all the law enforcement measures into the security services. However, such safeguards are clearly not designed for, and do not provide, an appropriate or proportionate basis for the unique nature of intelligence services processing, which we are clear is outside the scope of EU law.

Before I get into the detail of these amendments, it is important to put on record that the international transfer of personal data is vital to the intelligence services’ ability to counter threats to national security. Provision of data to international partners bolsters their ability to counter threats to their security and that of the UK. In a globalised world, threats are not necessarily contained within one country, and the UK cannot work in isolation. As terrorists do not view national borders as a limit to their activities, the intelligence services must be in a position to operate across borders and share information quickly—for example, about the nature of the threat that an individual poses—to protect the UK.

In the vast majority of cases, intelligence sharing takes place with countries with which the intelligence services have long-standing and well-established relationships.
In all cases, however, the intelligence services apply robust necessity and proportionality tests before sharing any information. The inherent risk of sharing information must be balanced against the risk to national security of not sharing such information.

Liam Byrne: Will the Minister tell us more about the oversight and scrutiny for the tests that she has just set out that the intelligence services operate? Perhaps she will come on to that.

Victoria Atkins: I am coming on to that.

Any cross-border sharing of personal data must be consistent with our international obligations and be subject to appropriate safeguards. On the first point, the provisions in clause 109 are entirely consistent with the requirements of the draft modernised Council of Europe data protection convention—convention 108—on which the provisions of part 4 are based. It is pending international agreement.

The provisions in the convention are designed to provide the necessary protection for personal data in the context of national security. The Bill already provides that the intelligence services can make transfers outside the UK only when necessary and proportionate for the limited purposes of the services’ statutory functions, which include the protection of national security; for the purpose of preventing or detecting serious crime; or for the purpose of criminal proceedings.

In addition, on the point the right hon. Gentleman just raised, the intelligence services are already under statutory obligations in the Security Service Act 1989 and the Intelligence Services Act 1994 to ensure that no information is disclosed except so far as is necessary for those functions or purposes. All actions by the intelligence services, as with all other UK public authorities, must comply with international law.

Louise Haigh (Sheffield, Heeley) (Lab): Will the Minister give way?

Victoria Atkins: Yes, but I am coming on to further safeguards, if that is the point the hon. Lady wants to raise.

Louise Haigh: Under those pieces of legislation, are the intelligence services subject to the Information Commissioner, and will they be subject to the commissioner under the Bill’s provisions?

Victoria Atkins: I am about to come on to the safeguards that govern the intelligence services’ information acquisition and sharing under the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000. They ensure that any such processing is undertaken only when necessary, lawful and proportionate, and that any disclosure is limited to the minimum number of individuals, in accordance with arrangements detailed in those Acts.

Those Acts, and the provisions in the relevant codes of practice made under them, also provide rigorous safeguards governing the transfer of data. Those enactments already afford proportionate protection and safeguards when data is being shared overseas. Sections 54, 130, 151 and 192 of the 2016 Act provide for safeguards relating to disclosure of material overseas.

Those provisions are subject to oversight by the investigatory powers commissioner, and may be challenged in the investigatory powers tribunal. They are very powerful safeguards, over and above the powers afforded to the Information Commissioner, precisely because of the unique nature of the material with which the security services must act.

Peter Heaton-Jones (North Devon) (Con): Is the point not that those who would seek to do us harm do not have the courtesy to recognise international borders, as recent events have shown? It is vital that our intelligence services can share information across those same borders.

Victoria Atkins: It is absolutely vital. What is more, not only is there a framework in the Bill for overseeing the work of the intelligence services, but we have the added safeguards of the other legislation that I set out. They burden on the security services and the thresholds they have to meet are very clear, and they are set out not just in the Bill but in other statutes.

I hope that I have provided reassurance that international transfers of personal data by the intelligence services are appropriately regulated both by the Bill, which, as I said, is entirely consistent with draft modernised convention 108 of the Council of Europe—that is important, because it is the international agreement that will potentially underpin the Bill and agreements with our partners and sets out agreed international standards in this area—and by other legislation, including the 2016 Act. We and the intelligence services are absolutely clear that to attempt to impose, through these amendments, a regime that was specifically not designed to apply to processing by the intelligence services would be disproportionate and may critically damage national security.

I am sure that it is not the intention of the right hon. Member for Birmingham, Hodge Hill to place unnecessary and burdensome obstacles in the way of the intelligence services in performing their crucial function of safeguarding national security, but, sadly, that is what his amendments would do. I therefore invite him to withdraw them.

Liam Byrne: I am grateful to the Minister for that explanation and for setting out with such clarity the regime of oversight and scrutiny that is currently in place. However, I have a couple of challenges.

I was slightly surprised that the Minister said nothing about the additional risks created by the change in rules of engagement by the United States. She rested some of her argument on the Security Services Act 1989 and the Intelligence Services Act 1994, which, as she said, require that any transfers of information are lawful and proportionate. That creates a complicated set of ambiguities for serving frontline intelligence officers, who have to make fine judgments and, in drafting codes of practice, often look at debates such as this one and at the law. However, the law is what we are debating. Where the Bill changed the law to create a degree of flexibility, it would create a new risk, and that risk would be heightened by the change in the rules of engagement by one of our allies.
The Minister may therefore want to reflect on a couple of points. First, what debate has there been about codes of practice? Have they changed given the increased surveillance capacity that we have because of the development of our capabilities? How have they changed in the light of the new rules of engagement issued by President Trump?

Peter Heaton-Jones: The right hon. Gentleman is being generous in giving way. I am listening carefully to what he says. I am concerned that he seems to be inviting us to make law in this country based almost solely on the policies of the current US Administration. I do not understand why we would do that.

Liam Byrne: The reason we would do that is that there has been an exponential increase in drone strikes by President Trump’s Administration and, as a result, a significant increase in civilian deaths in Pakistan, Afghanistan, Syria and Iraq, Yemen and east Africa. It would be pretty odd for us not to ensure that a piece of legislation had appropriate safeguards, given what we now know about the ambition of one of our most important allies to create flexibility in rules of engagement.

Matt Warman (Boston and Skegness) (Con): I agree with the right hon. Gentleman on that point, but is not the more important point that our legislation cannot be contingent on that of any other country, however important an ally it is? Our legislation has to stand on its own two feet, and we should seek to ensure that it does. To change something, as he attempts to, purely on the basis of changes over the past couple of years would set a dangerous precedent rather than guard against a potential pitfall.

10.15 am

Liam Byrne: The hon. Gentleman makes a good point, and he is right to say that our legislation has to stand on its own two feet. It absolutely has to, and what is more, it has to be fit for the world in which we live today, which I am afraid has two significant changes afoot. One is a transformation in the power of our intelligence agencies to collect and process data, and in my view that significant advance is enough to require a change in the level of oversight, and potentially a judicial test for the way we share information. As it happens—I was careful to say this—the risk and necessity of that change is merely heightened by the fact that the rules of engagement with one of our most important allies have changed, and that has had real-world consequences. Those consequences create a heightened threat of legal challenge in foreign and indeed domestic courts to our serving personnel.

For some time, our defence philosophy has been—very wisely—that we cannot keep our country safe by defending from the goal line, and on occasion we have to intervene abroad. That is why in my view Prime Minister Cameron took the right decision to authorise lethal strikes against two British citizens. He was concerned first that there was an imminent threat, and secondly that there was no other means of stopping them. Those important tests and safeguards are not operated by our allies.

The change to the American rules of engagement, which allow a strike against someone who is no longer a “continuing and imminent threat”, means that one of our allies now operates under completely different rules of engagement to those set out before the House of Commons by Prime Minister David Cameron, which I think met with some degree of approval. If we are to continue to operate safely a policy of not defending from the goal line, if we are to protect our ability to work with allies and—where necessary and in accordance with international law—to take action abroad, and if we are to continue the vital business of safely sharing information with our allies in the Five Eyes network, a degree of extra reassurance should be built into legislation to ensure that it is fit for the future.

Mr Alister Jack (Dumfries and Galloway) (Con): I am confused. Is the right hon. Gentleman suggesting that the actions by Americans, based on the data sharing, which we know is run with international safeguards, could have legal consequences for our personnel in the intelligence agencies serving here?

Liam Byrne: Yes, and it is not just me—the Court of Appeal is arguing that. The Court of Appeal’s summary in 2013 was that there was a risky legal ambiguity. Its conclusion that it is certainly not clear that UK personnel are immune from criminal liability for their involvement in these programmes is a concern for us all. The Joint Committee on Human Rights reflected on that in 2016, and it concluded pretty much the same thing:

“In our view, we owe it to all those involved in the chain of command for such uses of lethal force...to provide them with absolute clarity about the circumstances in which they will have a defence against any possible future criminal prosecution, including those which might originate from outside the UK.”

This is not a theoretical legal threat to our armed forces and intelligence agencies; this is something that the Court of Appeal and the Joint Committee on Human Rights have expressed worries about.

The new powers and capabilities of our intelligence agencies arguably create the need for greater levels of oversight. This is a pressing need because of the operational policy of one of our allies. We owe it to our armed forces and intelligence agencies to ensure a regime in which they can take clear, unambiguous judgments where possible, and where they are, beyond doubt, safe from future legal challenge. It is not clear to me that the safeguards that the Minister has set out meet those tests.

Perhaps the Minister will clarify one outstanding matter, about convention 108, on which she rested much of her argument. Convention 108 is important. It was written in 1981. The Minister told the Committee that it had been modernised, but also said that that was in draft. I should be grateful for clarification of whether the United Kingdom has signed and is therefore bound by a modernised convention that is currently draft.

Victoria Atkins: I am happy to clarify that. Convention 108 is in the process of being modernised by international partners. I have made it clear, last week and this week, that the version in question is modernised, and is a draft version; but it is the one to which we are committed, not least because the Bill reflects its provisions. Convention 108 is an international agreement and sets the international standards, which is precisely why we are incorporating those standards into the Bill.

I know that the Leader of Her Majesty’s Opposition appears to be stepping away from the international community, over the most recent matters to do with Russia, but the Bill and convention... [Interruption.]
Well, he is. However, convention 108 is about stepping alongside our international partners, agreeing international standards and putting the thresholds into legislation. The right hon. Gentleman keeps talking about the need for legislation fit for the world we live in today; that is precisely what convention 108 is about.

**The Chair:** Order. The right hon. Member for Birmingham, Hodge Hill indicates that this is an intervention. I thought he had sat down and wanted the Minister to respond. However, if it is an intervention, it is far too long.

**Liam Byrne:** I am grateful. Some of us in this House have been making the argument about the risk from Russia for months, and the permissive environment that has allowed the threats to multiply is, I am afraid, the product of much of the inattention of the past seven years.

On the specific point about convention 108, I am glad that the Minister has been able to clarify the fact that it is not operational.

**Victoria Atkins:** On the language—

**Liam Byrne:** I will give way to the Minister in a moment. The convention was written in 1981. Many people in the Government have argued in the past that we should withdraw not only from the European Union but from the European convention on human rights and therefore also the Council of Europe.

**Victoria Atkins:** That is not Government policy.

**Liam Byrne:** I did not say it was Government policy. I said that there are people within the Administration, including the Secretary of State for Environment, Food and Rural Affairs, who have made the argument for a British Bill of Rights that would remove Britain from the European convention on human rights and, therefore, the Council of Europe. I very much hope that that ambiguity has been settled and that the policy of the current Government will remain that of the Conservative party from now until kingdom come; but the key point for the Committee is that convention 108 is in draft. The modernisation is in draft and is not yet signed. We have heard an express commitment from the Minister to the signing of the thing when it is finalised. We hope that she will remain in her position, to ensure that that will continue to be Government policy; but the modernised version that has been drafted is not yet a convention.

**Darren Jones:** Does my right hon. Friend recognise that the modernisation process started in 2009, with rapporteurs including one of our former colleagues, Lord Prescott? When a process has taken quite so many years and the document is still in draft, it raises the question of how modern the modernisation is.

**Liam Byrne:** Some members of the Committee—I am one of them—have been members of the Parliamentary Assembly of the Council of Europe for some time. We know how the Council of Europe works. It is not rapid: it likes to take its time deliberating on things. The Minister may correct me, but I do not think that there is a deadline for the finalisation of the draft convention. So, to ensure that the Government remain absolutely focused on the subject, we will put the amendment to a vote.

**Question put.** That the amendment be made.

**The Committee divided: Ayes 9, Noes 10.**

**Division No. 8**

**AYES**

Byrne, rh Liam
Elmore, Chris
Heigh, Louise
Jones, Darren
McDonald, Stuart C.

**NOES**

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

Question accordingly negatived.

Clause 109 ordered to stand part of the Bill.

Clauses 110 to 112 ordered to stand part of the Bill.

Schedule 11

**OTHER EXEMPTIONS UNDER PART 4**

**Amendments made:** 118, in schedule 11, page 190, line 4, leave out “day falls before the day on which” and insert “time falls before”.

This amendment is consequential on Amendment 71.

Amendment 119, in schedule 11, page 190, line 7, leave out “day” and insert “time”.

This amendment is consequential on Amendment 71.

Amendment 120, in schedule 11, page 190, line 9, leave out “the date of”.

This amendment is consequential on Amendment 71.

Amendment 121, in schedule 11, page 190, line 17, leave out “day” and insert “time”.—(Victoria Atkins.)

This amendment is consequential on Amendment 71.

Schedule 11, as amended, agreed to.

**Clause 113**

**POWER TO MAKE FURTHER EXEMPTIONS**

**Question proposed.** That the clause stand part of the Bill.

**Stuart C. McDonald:** Clause 113 is one of the broad Henry VIII powers that we are consistently opposing and voting against and will continue to oppose and vote against. In chapter 6 of part 4 of the Bill are set out various exemptions that would disapply a number of aspects of data protection if that were required for national security. In schedule 11 are set out further exemptions, including for prevention and detection of crime, parliamentary privilege, legal professional privilege and so on. Huge swathes of data protection principles and subjects’ rights disappear in those circumstances.
We have already had a number of good debates on whether we have struck the right balance between the rights of data subjects and the national interest, national security interests and so on. In our view, it rather undermines our role in scrutinising Government legislation and finding the right balance if we then hand over what is pretty much a carte blanche to change the balance that we have decided on, with the minimum of scrutiny, through broad Henry VIII powers. We therefore continue to oppose broad Henry VIII powers in the Bill and encourage hon. Members to support taking this clause out of the Bill.

Victoria Atkins: I thank the hon. Gentleman for raising this point. Clause 113 is analogous to clause 16, which we have already debated, and provides for the Secretary of State, by regulations subject to the affirmative procedure, to add further exemptions from the provisions of part 4 or to omit exemptions added by regulations. This clause reflects amendments made in the House of Lords in response to the Delegated Powers and Regulatory Reform Committee’s concerns that the powers in the Bill as introduced, which provided for adding, varying or omitting further exemptions in relation to schedule 11, were inadequately justified and too widely drawn. However, maintaining the power to add further exemptions, or to omit exemptions that have been added, provides the flexibility required, if necessary, to extend exemptions in the light of changing public policy requirements.

10.30 am

Any regulations will be subject to the affirmative procedure, so they will have to be debated and approved by both Houses. I hope that gives the hon. Gentleman some comfort. In addition, clause 179 requires the Home Secretary to consult the Information Commissioner and other interested parties that they consider appropriate before bringing forward any regulations. Again, those are further procedural safeguards.

Question put and agreed to.

Clause 113 accordingly ordered to stand part of the Bill.

Clause 114 ordered to stand part of the Bill.

Schedule 12 agreed to.

Clauses 115 and 116 ordered to stand part of the Bill.

Schedule 13

Other general functions of the Commissioner

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): I beg to move amendment 122, in schedule 13, page 194, line 36, leave out from beginning to end of line 4 on page 195.

This amendment is consequential on the omission of Clause 121 (see Amendment 47).

The Chair: With this it will be convenient to discuss clause 121 stand part.

Margot James: Amendment 122 and clause 121 deal with measures inserted into the Bill with the intention of protecting and valuing certain personal data held by the state—an issue championed by Lord Mitchell, to whom I am grateful for taking the time to come to see me to further explain his amendments, and for giving me the opportunity to explain how we plan to address the issues he raised.

Lord Mitchell’s amendments require the Information Commissioner to maintain a register of publicly controlled data of national significance and to prepare a code of practice that contains practical guidance in relation to personal data of national significance, which is defined as data that, in the Commissioner’s opinion,

“has the potential to further...economic, social or environmental well-being”

and

“financial benefit...from processing the data or the development of associated software.”

Lord Mitchell has made it clear that his primary concern relates to the sharing of health data by the NHS with third parties. He believes that some information sharing agreements have previously undervalued NHS patient data, and that the NHS, along with other public authorities, needs additional guidance on optimising the benefits derived from such sharing agreements.

We agree that the NHS is a prime state asset, and that its rich patient data records have great potential to further medical research. Its data could be used to train systems using artificial intelligence to diagnose patients’ conditions, to manage risk, to target services and to take pre-emptive and preventive action—all developments with huge potential. I have discussed this matter with ministerial colleagues; not only do we want to see these technological developments, but we want the NHS, if it is to make any such deals, to make fair deals. The benefits of such arrangements are often not exclusively monetary.

NHS patient data is only ever used within the strict parameters of codes of practice and the standards set out by the National Data Guardian and other regulatory bodies. We of course recognise that we must continue in our efforts to make the best use of publicly held data, and work is already being carried out to ensure that the value of NHS patient data is being fully recognised. NHS England and the Department of Health and Social Care have committed to working with representatives of the public and of industry to explore how to maximise the benefits of health and care data for patients and taxpayers.

Lord Mitchell’s provision in clause 121 proposes that the commissioner publish a code of practice. However, if there is a problem, a code would seem to be an unduly restrictive approach. Statutory codes are by necessity prescriptive, and this is an area where the public may benefit from a greater degree of flexibility than a code could provide in practice, especially to encourage innovation in how Government use data to the benefit of both patients and taxpayers.

The Government are releasing public data to become more transparent and to foster innovation. We have released more than 40,000 non-personal datasets. Making the data easily available means that it will be easier for people to make other uses of Government-collected data, including commercial exploitation or to better understand how government works and to hold the Government to account. The benefits of each data release are quite different, and sometimes they are unknown until later. Lord Mitchell’s primary concern is
health data, but can guidance on how that is used be equally applicable to the vast array of data we release? Such guidance would need to be so general that it would be useless.

Even if we stay focused on NHS data and what might help to ensure that the value of it is properly exploited, Lord Mitchell’s proposal has some significant problems. First, by definition, data protection legislation deals with the protection of personal data, not general data policy. Companies who enter into data sharing agreements with the NHS are often purchasing access to anonymised patient data—that is to say, not personal data. Consequently, the code in clause 121 cannot bite. Secondly, maintaining a register of data of national significance is problematic. In addition to the obvious bureaucratic burden of identifying the data that would fall under the definition, generating a list of data controllers who hold data of national significance is likely to raise a number of security concerns. The NHS has been the victim of cyber-attacks, and we do not want to produce a road map to resist those who want to harm it.

Thirdly, we do not believe that the proposed role is a proper one for the Information Commissioner, and nor does she. It is not a question of legislative enforcement and, although she may offer valuable insight on the issues, such responsibilities do not comfortably fit with her role as regulator of data protection legislation. We have consulted the commissioner on the amendments and she agrees with our assessment. In her own terms, she considers herself not to be best placed to advise on value for money and securing financial benefits from the sharing of such personal data with third parties. Those matters are far removed from her core function of safeguarding information rights. She adds that others in Government or the wider public sector whose core function it is to drive value from national assets may be a more natural home for providing such best practice advice.

Ian Murray (Edinburgh South) (Lab): I have the great pleasure of representing a constituency with one of the best medical research facilities in the world. One of the greatest impediments for that facility is getting access to anonymised NHS data for its research. Is the Minister saying that her amendment, which would remove the Lords amendment, would make it easier or more difficult for third parties to access that anonymised data?

Margot James: I am ill-qualified to answer the hon. Gentleman’s question. Hypothetically, it would probably make it more difficult, but that is not our purpose in objecting to clause 121, which we do not see as being consistent with the role of the Information Commissioner, for the reasons I set out. However, he raises an interesting question.

I agree with Lord Mitchell that the issues that surround data protection policy, particularly with regard to NHS patient data, deserve proper attention both by the Government and by the National Data Guardian for Health and Care, but we have not yet established that there is a problem to which his provisions are the answer. We are not sitting on our laurels. As I have already said, NHS England and the Department of Health and Social Care are working to ensure that they understand the value of their data assets. Further work on the Government’s digital charter will also explore this issue. When my right hon. friend the Prime Minister launched the digital charter on 25 January, she made it clear that we will set out principles on the use of personal data.

Amendment 122 removes Lord Mitchell’s amendment from schedule 13. We do this because it is the wrong tool; however, we commit to doing everything we can to ensure that we further explore the issue and find the right tools if needed. [Interruption.] I have just received advice that the amendments will make no difference in relation to the hon. Gentleman’s question, because anonymised data is not personal data.

I commend amendment 122 and give notice that the Government will oppose the motion that clause 121 stand part of the Bill.

Liam Byrne: I am grateful that the Minister made time to meet my former noble Friend Lord Mitchell. These are important amendments and it is worth setting out the background to why Lord Mitchell moved them and why we give such priority to them.

In 2009-10, we began to have a debate in government about the right approach to those agencies which happen to sit on an enormous amount of important data. The Government operate about 200 to 250 agencies, and some are blessed with data assets that are more valuable than those of others—for example, the Land Registry or Companies House sit on vast quantities of incredibly valuable transactional data, whereas other agencies, such as the Meteorological Office, the Hydrographic Office and Ordnance Survey, sit on sometimes quite static data which is of value. Some of the most successful American companies are based on Government data—for example, The Weather Channel is one of the most valuable and is based on data issued from, I think, the US meteorological survey. A number of Government agencies are sitting on very valuable pots of data.

The debate that we began to rehearse nearly 10 years ago was whether the right strategy was to create public-private partnerships around those agencies, or whether more value would be created for the UK economy by simply releasing that data into the public domain. I had the great pleasure of being Chief Secretary to the Treasury and the Minister for public service reform. While the strong advice inside the Treasury was that it was better to create public-private partnerships because that would release an equity yield up front, which could be used for debt reduction, it was also quite clear to officials in the Cabinet Office and those interested in public service reform more generally that the release of free data would be much more valuable. That is the side of the argument on which we came down.

After the White Paper, “Smarter Government”, that I brought to the House, we began the release of very significant batches of data. We were guided by the arguments of Tim Berners-Lee and Professor Nigel Shadbolt, who were advising us at the time, that this was the right approach and it was very good to see the Government continue with that.

There are still huge data pots locked up in Government which could do with releasing, but the way in which we release them has to have an eye on the way we create value for taxpayers more generally. Beyond doubt, the
area of public policy and public operations where we have data that is of the most value is health. The way in which, in the United States, Apple and other companies have now moved into personal health technology in a substantial way betrays the reality that this is going to be a hugely valuable and important market in years to come. If we look at the US venture industry we can see significant investment now going into health technology companies.

10.45 am

Lord Mitchell’s amendment is designed to steer the Government in a particular direction. He would be the first to accept that it is imperfect and that the Information Commissioner is not the perfect custodian of the task, but the question is: how do we make progress and why is this so important? It is important because the Government have made mistakes in the way they have thought about the value of intellectual property in some of the joint ventures they have created in the last seven years. Let us look, for example, at the Government’s approach to Hinkley Point and the investment it sought from Chinese investors. Frankly, the Chinese cannot believe the structure of the deal because it is so generous to Chinese investors. A huge amount of investment is sought to modernise the nuclear industry in one of the most important economies in the world, and all the intellectual property flows back to the Chinese investors. If the deal were being set up in France or Germany, or indeed in China, it would be set up as a joint venture in which the intellectual property rights were invested in the joint venture, and the Government were therefore a party who would enjoy the upside of the use of that data in the future.

What Lord Mitchell is super-conscious of is that our NHS records stretch back to 1948, so the longitudinal health data we have in this country is pretty much without parallel anywhere in the world. Some regions, such as the NHS in the west midlands, operate an extremely extensive payer database of the use of medications in a super-diverse population. The dynamic and longitudinal data assets that we are sitting on in parts of the NHS are unbelievably valuable. In the arguments he rehearsed in the other place, Lord Mitchell made the point that the data the NHS is sitting on is like our North sea oil—in fact, it is probably more valuable than the North sea oil assets discovered in the early 1970s. He has told me that at least two sources have related to him that the annual value of those longitudinal data records is of the order of £50 billion. I cannot vouch for that figure or for the source, but I know Lord Mitchell has done his homework on this. He is seeking to ensure that something almost like a sovereign wealth fund is created for data assets in this country—in particular, a sovereign wealth fund created for NHS data assets.

We would like to avoid the kind of mistakes that were made in assembling the Hinkley Point joint venture. Lord Mitchell’s amendment is quite simple: he seeks the creation of a register of significant data assets. The Minister says it is difficult to put that together, but life is a bit difficult sometimes. That is why we have highly paid Ministers and poorly paid officials, to work together to assemble the arguments and the data.

The precedent we have is back in, I think, 1998-99, when the last Labour Government put together what came to be called the Domesday book of Government assets. We are now looking for a similar kind of catalogue assembled for significant data assets. Rather unflatteringly for a Labour MP, at that time I was an investment banker working for a small bank called Rothschild & Co. in London. I know that will ruin my pro-Corbyn credentials.

Margot James: They were never very impressive.

Liam Byrne: The Minister is very generous. From that vantage point in the City, I was able to watch the level of ingenuity, creativity and innovation that was unlocked simply by the Government telling the world, “Here are the assets that are in public hands.” All sorts of ideas were floated for using those assets in a way that was better for taxpayers and public service delivery.

To the best of my knowledge, we do not have a similar data catalogue today. What Lord Mitchell is asking is for Ministers to do some work and create one. They can outsource that task to the Information Commissioner. Perhaps the Information Commissioner is not the best guardian of that particular task, but I am frustrated and slightly disappointed that the Minister has not set out a better approach to achieving the sensible and wise proposals that Lord Mitchell has offered the Government.

The reason why it is so important in the context of the NHS is that the NHS is obviously a complicated place. It is an economy the size of Argentina’s. The last time I looked, if the NHS were a country, it would be the 13th biggest economy on earth. It is a pretty complicated place and there are many different decision makers. Indeed, there are so many decision makers now that it is impossible to get anything done within the NHS, as any constituency MP knows. So how do we ensure that, for example, in our neck of the woods, Queen Elizabeth Hospital Birmingham does not strike its own data sharing agreement with Google or DeepMind? How do we ensure that the NHS in Wales does not go in a particular direction? How do we ensure that the trust across the river does not go in a particular direction? We need to bring order to what is potentially an enormously missed opportunity over the years to come.

The starting point is for the Government, first, to ensure we have assembled a good catalogue of data assets. Secondly, they should take some decisions about whether the organisations responsible for those data assets are destined for some kind of public-private partnership, as they were debating in relation to Companies House and other agencies a couple of years ago, or whether—more wisely—we take the approach of creating a sovereign wealth fund to govern public data in this country, where we maximise the upside for taxpayers and the opportunities for good public service reform.

The example of Hinkley Point and the unfortunate example of the Google partnership with DeepMind, which ran into all kinds of problems, are not good precedents. In the absence of a better, more concrete, lower risk approach from the Government, we will have to defend Lord Mitchell’s wise clause in order to encourage the Government to come back with a better solution than the one set out for us this morning.

Margot James: I enjoyed the right hon. Gentleman’s speech, as it went beyond some of the detail we are debating here today, but I was disappointed with the
conclusion. I did not rest my argument it being just too difficult to organise such a database as proposed by Lord Mitchell; there are various reasons, chief among them being that we are here to debate personal data. A lot of the databases the right hon. Gentleman referred to as being of great potential value do not contain personal data. Some do, some do not: the Land Registry does not, Companies House does, and so forth. Also, the Information Commissioner has advised that this is beyond her competence and her remit and that she is not resourced to do the job. Even the job of defining what constitutes data of public value is a matter for another organisation and not the Information Commissioner’s Office. That is my main argument, rather than it being too difficult.

Liam Byrne: Happily, what sits within the scope of a Bill is not a matter for Ministers to decide. First, we rely on the advice of parliamentary counsel, which, along with the Clerks, was clear that this amendment is well within the scope. Secondly, if the Information Commission is not the right individual to organise this task—heaven knows, she has her hands full this week—we would have been looking for a Government amendment proposing a better organisation, a better Ministry and a better Minister for the work.

Margot James: I can only be the Minister I am. I will try to improve. I was not saying that Lord Mitchell’s amendment is not within the scope of the Bill; I was making the point that some of the databases and sources referred to by the right hon. Gentleman in his speech went into the realms of general rather than personal data. I therefore felt that was beyond the scope of the Information Commissioner’s remit.

I share the right hon. Gentleman’s appreciation of the value and the uniqueness of the NHS database. We do not see it just in terms of its monetary value; as the hon. Member for Edinburgh South made clear in his intervention, it has tremendous potential to improve the care and treatment of patients. That is the value we want to realise. I reassure the right hon. Gentleman and put it on record that it is not my place as a Minister in Department for Digital, Culture, Media and Sport, or the place of the Bill, to safeguard the immensely valuable dataset that is the NHS’s property.

Louise Haigh: Before the Minister concludes, given that she has focused so much on NHS data, can she update the Committee on the Government’s progress on implementing Dame Fiona Caldicott’s recommendations about health and social care data?

Margot James: I cannot give an immediate update on that, but I can say that Dame Fiona Caldicott’s role as Data Guardian is crucial. She is working all the time to advise NHS England and the Secretary of State for Health and Social Care on how best to protect data and how it can deliver gains in the appropriate manner. I do not feel that that is the place of the Bill or that it is my role, but I want to reassure the Committee that the Secretary of State for Health and Social Care, to whom I am referring Lord Mitchell, is alive to those issues and concerns. The NHS dataset is a matter for the Department of Health and Social Care.

Amendment 122 agreed to.
Schedule 13, as amended, agreed to.
Clauses 117 and 118 ordered to stand part of the Bill.
Schedule 14 agreed to.
Clauses 119 and 120 ordered to stand part of the Bill.

Clause 121

CODE ON PERSONAL DATA OF NATIONAL SIGNIFICANCE

11 am

The Chair: We debated clause 121 with schedule 13. For those who are interested, the Minister proposed that the clause should not stand part of the Bill, but the question remains “That the clause stand part of the Bill.” For the avoidance of confusion—I have only been here 26 years—those who, like the Minister, do not want the clause to stand part of the Bill should vote no.

Question put, That the clause stand part of the Bill.

The Committee divided: Ayes 9, Noes 10.

Division No. 9

AYES

Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren
McDonald, Stuart C.

Murray, Ian
O’Hara, Brendan
Snell, Gareth
Zeichner, Daniel

NOES

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel
Jack, Mr Alister
James, Margot
Lopez, Julia
Warman, Matt
Wood, Mike

Question accordingly negatived.

Clause 121 disagreed to.

Clauses 122 and 123 ordered to stand part of the Bill.

Clause 124

AGE-APPROPRIATE DESIGN CODE

Amendment made: 48, in clause 124, page 68, line 24, leave out “with the day on which” and insert “when”.

This amendment is consequential on Amendment 71.—[Margot James]

Question proposed, That the clause, as amended, stand part of the Bill.

Liam Byrne: The debate rehearsed in the other place was whether we should acquiesce in a derogation that the Government have exercised to set the age of consent for personal data sharing at 13, as opposed to 16, which other countries have adopted. There was widespread concern that 13 was too young. Many members of the Committee will have experienced pressing the agree button when new terms and conditions are presented to us on our updates to software on phones, or privacy
settings presented to us by Facebook; privacy settings, it is now alleged, are not worth the paper that they were not written on.

Debates in the other place centred on what safeguards could be wrapped around children if that derogation were exercised and the age of consent left at 13. With Baroness Kidron, we were keen to enshrine in legislation a step towards putting into operation the objectives of the 5Rights movement. Those objectives, which Baroness Kidron has driven forward over the past few years, are important, but the rights therein are also important. They include not only rights that are enshrined in other parts of the Bill—the right to remove, for example—but important rights such as the right to know. That means that someone has the right to know whether they are being manipulated in some way, shape or form by social media technologies.

One of the most interesting aspects of the debate in the public domain in the past few months has been the revelation that many of the world’s leading social media entrepreneurs do not allow their children to use social media apps, because they know exactly how risky, dangerous and manipulative they can be. We have also heard revelations from software engineers who used to work for social media companies about the way they deliberately set out to exploit brain chemistry to create features of their apps that fostered a degree of addiction. The right to know is therefore very powerful, as is the right to digital literacy, which is another important part of the 5Rights movement.

It would be useful to hear from the Minister of State, who—let me put this beyond doubt—is an excellent Minister, what steps she plans to take to ensure that the age-appropriate design code is set out pretty quickly. We do not want the clause to be passed but then find ourselves in a situation akin to the one we are in with section 40 of the Crime and Courts Act 2013 where, five years down the line, a misguided Secretary of State decides that the world has changed completely and that this bit of legislation should not be commenced.

We would like the Minister to provide a hard timetable—she may want to write to me if she cannot do so today—setting out when we will see an age-appropriate design code. We would also like to hear what steps she will take to consult widely on the code, what work she will do with her colleagues in the Department for Education to ensure that the code includes some kind of ventilation and education in schools so that children actually know what their rights are and know about the aspects of the code that are relevant to them, and, crucially, what steps she plans to take to include children in her consultation when she draws up the code.

This is an important step forward, and we were happy to support it in the other place. We think the Government should be a little more ambitious, which is why we suggest that the rights set out by the 5Rights movement should become part of a much broader and more ambitious digital Bill of Rights for the 21st century, but a start is a start. We are pleased that the Government accepted our amendment, and we would all be grateful if the Minister told us a little more about how she plans to operationalise it.

Margot James: I thank the right hon. Gentleman for his generous remarks. To recap, the idea that everyone should be empowered to take control of their data is at the heart of the Bill. That is especially important for groups such as children, who are likely to be less aware of the risks and consequences associated with data processing. Baroness Kidron raised the profile of this issue in the other place and won a great deal of support from peers on both sides of that House, and the Government then decided to introduce a new clause on age-appropriate design to strengthen children’s online rights and protections.

Clause 124 will require the Information Commissioner to develop a new statutory code that contains guidance on standards of age-appropriate design for online services that are likely to be accessed by children. The Secretary of State will work in close consultation with the commissioner to ensure that that code is robust, practical and meets children’s needs in relation to the gathering, sharing and storing of their data. The new code will ensure that websites and apps are designed to make clear what personal data of children is collected, how it is used and how both children and parents can stay in control of it. It will also include requirements for websites and app makers on privacy for children under 18.

The right hon. Gentleman cited examples of the consultation he hopes to see in preparation for the code. In developing the code, we expect the Information Commissioner to consult a wide range of stakeholders, including children, parents, persons who represent the interests of children, child development experts and trade associations. The right hon. Gentleman mentioned the Department for Education, and I see no reason why it should not be included in that group of likely consultees.

The commissioner must also pay close attention to the fact that children have different needs at different ages, as well as to the United Kingdom’s obligations under the United Nations Convention on the Rights of the Child. The code interlocks with the existing data protection enforcement mechanism found in the Bill and the GDPR. The Information Commissioner considers many factors in every regulatory decision, and non-compliance with that code will weigh particularly heavily on any organisation that is non-compliant with the GDPR. Organisations that wish to minimise their risk will apply the code. The Government believe that clause 124 is an important and positive addition to the Bill.

Liam Byrne: Will the Minister say a word about the timetable? When can we expect the consultation and code of practice to be put into operation?

Margot James: There should be no delay to the development of the code and the consultation that precedes it. If I get any additional detail on the timetable, I will write to the right hon. Gentleman.

Question put and agreed to.

Clause 124, as amended, ordered to stand part of the Bill.

Clause 125

APPROVAL OF DATA-SHARING, DIRECT MARKETING AND AGE-APPROPRIATE DESIGN CODES

Amendment made: 49, in clause 125, page 69, line 9, leave out “with the day on which” and insert “when” — (Margot James.)

This amendment is consequential on Amendment 71.

Clause 125, as amended, order to stand part of the Bill.

Clauses 126 to 130 ordered to stand part of the Bill.
Clause 131

Disclosure of Information to the Commissioner

Question proposed, That the clause stand part of the Bill.

Liam Byrne: Clause 131 deals with disclosure of information to the Information Commissioner, and this is probably a good point at which to ask whether the Information Commissioner has the right level of power to access information that is pertinent to her investigations into the misuse of information. Thanks to The Guardian, The New York Times, and particularly the journalist Carole Cadwalladr, we have had the most extraordinary revelations about alleged misdemeanours at Cambridge Analytica over the past couple of years. Indeed, Channel 4 News gave us further insight into its alleged misdemeanours last night.

We have a situation in social media land that the Secretary of State has described as the “wild west”. Some have unfairly called the Matt Hancock app one of the features of that wild west, but I would not go that far, despite its slightly unusual privacy settings. None the less, there is now cross-party consensus that the regulatory environment that has grown up since the 2000 e-commerce directive is no longer fit for purpose. Yesterday, the Secretary of State helpfully confirmed that that directive will be modernised, and we will come on to discuss new clauses that suggest setting a deadline for that.

One deficiency of today’s regulatory environment is the inadequate power that the Information Commissioner currently has to access information that is important for her investigations. We have a wild west, we have hired a sheriff, but we have not given the sheriff the power to do her job of keeping the wild west in order. We now have the ridiculous situation that the Information Commissioner must declare that she is going to court to get a warrant to investigate the servers of Cambridge Analytica, and to see whether any offence has been committed.

11.15 am

The offence is potentially incredibly serious. We are talking about data collected through an app called “My Digital World” that ran on Facebook and allowed the individuals in question to collect data on around 50 million people. Certainly, 50 million data records were assembled for a particular purpose. The allegation is that the data was then repurposed by Cambridge Analytica and put in the service of winning election campaigns, including the election of the President of the United States. This is not immaterial, and it is not a trivial offence or a public policy question. We should not glide over it, shrug our shoulders and say, “Well that is just part and parcel of the new world we live in.” This is something we should take incredibly seriously.

The way in which Facebook has, quite frankly, stonewalled investigations by this House through the excellent Department for Digital, Culture, Media and Sport Select Committee is all the more concerning. Essentially, Facebook told Members of this House that they were unable to check on allegations because they did not know what records to go and check. A company that makes a profit of $4 billion every single quarter has said to the House that it was unable to find the resources to investigate the kind of misdemeanours that have now been laid at their door and that of Cambridge Analytica.

I am concerned that the way our regulators operate together is simply inadequate. Many of the allegations about misuse of data during election campaigns and referendums will touch on whether the data was collected, repurposed illegally and then used to target so-called dark social ads in an inappropriate way, but there is also sometimes a need to explore where the money came from to buy those ads. Where money has, potentially, been laundered onshore there is a requirement for the Financial Conduct Authority to investigate. Sometimes it will require further investigations in, for example, Financial Conduct Authority countries such as Gibraltar.

At the moment, there is no information sharing gateway between the Financial Conduct Authority, the Electoral Commission and the Information Commissioner. It is actually impossible for any regulator to create a single picture of what on earth has gone on. That challenge gets even harder when the Information Commissioner does not have the power to get the information she needs to do her job.

Darren Jones: Does my hon. Friend agree that this is also a question of access to the judiciary? Last night, the Information Commissioner had to wait until this morning to get a warrant because no judges or emergency judges were available. At the same time, we assume that Facebook was able to exercise its contractual right to enter the offices of Cambridge Analytica. Emergency judges are available for terrorism or deportation cases. Should there not be access to emergency judges in cases of data misuse for quick regulatory enforcement too?

Liam Byrne: If I wanted to hide something from a newspaper and I thought that the newspaper was going to print it inappropriately, I would apply for an emergency injunction to stop the newspaper running it. I do not understand why the Information Commissioner has had to broadcast her intentions to the world, because that has given Cambridge Analytica a crucial period of time in which to do anything it likes, frankly, to its data records. The quality of the Information Commissioner’s investigation must be seriously impaired by the time that it has taken to get what is tantamount to a digital search warrant.

Is the Minister satisfied in her own mind that clause 131 and its associated clauses are powerful enough? Will she say more about the Secretary of State’s declaration to the House last night that he would be introducing amendments to strengthen the Commissioner’s power in the way that she requested? When are we going to see those amendments? Are we going to see them before this Committee rises, or at Report stage? Will there be a consultation on them? Is the Information Commissioner going to share her arguments for these extra powers with us and with the Secretary of State? We want to see a strong sheriff patrolling this wild west, and right now we do not know what the Government’s plan of action looks like.

Margot James: I just want to recap on what clause 131 is about. It is intended to make it clear that a person is not precluded by any other legislation from disclosing to the commissioner information that she needs in relation to her functions, under the Bill and other legislation. The only exception relates to disclosures prohibited by the Investigatory Powers Act 2016 on grounds of national security. It is therefore a permissive provision enabling people to disclose information to the commissioner.
However, the right hon. Member for Birmingham, Hodge Hill has taken the opportunity to question the powers that the Information Commissioner has at her disposal. As my right hon. Friend the Secretary of State said yesterday in the Chamber, we are not complacent. I want to correct something that the right hon. Member for Birmingham, Hodge Hill said. My right hon. Friend did not say that he would table amendments to the Bill on the matter in question. He did say that we were considering the position in relation to the powers of the Information Commissioner, and that we might table amendments, but we are in the process of considering things at the moment. I presume that that goes for the right hon. Gentleman as well; if not, he would surely have tabled his own amendments by now, but he has not.

Liam Byrne: The Minister will notice that I have tabled a number of new clauses that would, for example, bring election law into the 21st century. I think that the Secretary of State left the House with the impression yesterday that amendments to strengthen the power of the Information Commissioner would be pretty prompt. It is hard to see another legislative opportunity to put that ambition into effect, so perhaps the Minister will tell us whether we can expect amendments soon.

Margot James: I can certainly reassure the right hon. Gentleman that we are looking at the matter seriously and, although I cannot commit to tabling amendments, I do not necessarily rule them out. I have to leave it at that for now.

On a more positive note, we should at least acknowledge that, although the Bill strengthens the powers of the Information Commissioner, her powers are already the gold standard internationally. Indeed, we must bear it in mind that the data privacy laws of this country are enabling American citizens to take Cambridge Analytica to court over data breaches.

I want to review some of the powers that the Bill gives the commissioner, but before I do so I will answer a point made by the right hon. Member for Birmingham, Hodge Hill. He said that the commissioner had had difficulties and had had to resort to warrants to pursue her investigation into a political party in the UK and both the leave campaigns in the referendum. She is doing all that under existing data protection law, which the Bill is strengthening. That is encouraging.

Liam Byrne: I did not want to intervene, but I have been struggling with the matter myself. There are allegations that a significant donor to Leave.EU was supported in that financial contribution by organisations abroad. As I spoke to the Financial Conduct Authority and tabled questions to the Treasury, it was revealed that there were no data sharing gateways between the Electoral Commission and the FCA.

Margot James: I shall come back to the right hon. Gentleman on the relationship between the Information Commissioner and the FCA. I am sure that the information that he has already ascertained from the Treasury is correct, but there may be other ways in which the two organisations can co-operate, if required. The allegations are very serious and the Government are obviously very supportive of the Information Commissioner as she grapples with the current investigation, which has involved 18 information notices and looks as if it will be backed up by warrants as well. I remind the Committee that that is happening under existing data protection law, which the Bill will strengthen.

Question put and agreed to.

Clause 131 accordingly ordered to stand part of the Bill.

10.25 am

The Chair adjourned the Committee without Question put (Standing Order No. 88).

Adjourned till this day at Two o’clock.
CONTENTS

Clauses 132 to 141 agreed to.
Clause 142 disagreed to.
Clauses 143 to 153 agreed to, some with amendments.
Schedule 15 agreed to.
Clause 154 agreed to, with amendments.
Schedule 16 agreed to, with amendments.
Clauses 155 to 167, some with an amendment.
Clauses 168 and 169 disagreed to.
Clauses 170 to 181, one with an amendment.

Adjourned till Thursday 22 March at half-past Eleven o'clock.
Written evidence reported to the House.
No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Saturday 24 March 2018
The Committee consisted of the following Members:

**Chairs:** David Hanson, †Mr Gary Streeter

† Adams, Nigel (Lord Commissioner of Her Majesty’s Treasury)
† Atkins, Victoria (Parliamentary Under-Secretary of State for the Home Department)
† Byrne, Liam (Birmingham, Hodge Hill) (Lab)
† Clark, Colin (Gordon) (Con)
† Elmore, Chris (Ogmore) (Lab)
† Haigh, Louise (Sheffield, Heeley) (Lab)
† Heaton-Jones, Peter (North Devon) (Con)
† Huddleston, Nigel (Mid Worcestershire) (Con)
† Jack, Mr Alister (Dumfries and Galloway) (Con)
† James, Margot (Minister of State, Department for Digital, Culture, Media and Sport)

† Jones, Darren (Bristol North West) (Lab)
† Lopez, Julia (Hornchurch and Upminster) (Con)
† McDonald, Stuart C. (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP)
† Murray, Ian (Edinburgh South) (Lab)
† O’Hara, Brendan (Argyll and Bute) (SNP)
† Snell, Gareth (Stoke-on-Trent Central) (Lab/Co-op)
† Warman, Matt (Boston and Skegness) (Con)
† Wood, Mike (Dudley South) (Con)
† Zeichner, Daniel (Cambridge) (Lab)

Kenneth Fox, Committee Clerk

† attended the Committee
Public Bill Committee

Tuesday 20 March 2018

(Afternoon)

[Mr Gary Streeter in the Chair]

Data Protection Bill [Lords]

2 pm

Liam Byrne (Birmingham, Hodge Hill) (Lab): On a point of order, Mr Streeter. The Minister suggested this morning that the Secretary of State for Digital, Culture, Media and Sport had not committed to the House yesterday to introduce powers to strengthen the Information Commissioner. However, on checking Hansard over lunch, I noticed that the Secretary of State said that where there is non-compliance with an audit, “there is a very serious fine, but the question is whether the criminal penalties that can be imposed in some cases should be further strengthened. That detail is rightly being looked at in the discussions on the Data Protection Bill.”—[Official Report, 19 March 2018; Vol. 638, c. 51.]

Most of us would assume that “further strengthened” meant that further powers would be suggested, but the Minister seemed to say that that would not be the case. Could she clarify whether such amendments will be tabled?

The Chair: It is up to the Minister to decide whether she wishes to respond to that point of order.

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): I hesitated, Mr Streeter, because I am not quite sure that I can clarify the matter. I cannot answer the right hon. Gentleman’s question. I reiterate that in answer to the important question about strengthening the Information Commissioner’s powers, my right hon. Friend the Secretary of State said yesterday:

“We are therefore considering the Information Commissioner’s request.”—[Official Report, 19 March 2018; Vol. 638, c. 52.]

The right hon. Gentleman’s point was recently made by the commissioner, so it is a point worth listening to. I can confirm that we are listening and reviewing, but beyond that, I cannot go.

The Chair: As the Speaker himself might say, the right hon. Gentleman has been here a long time and will no doubt find other ways to pursue the matter. I am grateful for the point of order.

Clause 132 ordered to stand part of the Bill.

Clauses 133 to 139 ordered to stand part of the Bill.

Clause 140

Publication by the Commissioner

Question proposed, That the clause stand part of the Bill.

Margot James: I was not planning to speak to this clause, but as it is relevant I will use the opportunity to give the right hon. Member for Birmingham, Hodge Hill further information. He asked about the code of conduct where the commissioner has a responsibility to publish the document about child-friendly regulation of websites. Clause 140 provides that the document can be published in a way the commissioner considers appropriate. Under clause 126, the Bill contains a duty to publish various codes of practice, including the age-appropriate design code. The Bill requires the commissioner to publish the age-appropriate design code within 18 months of Royal Assent, but as the matter is important and urgent, we will endeavour to do so sooner.

Question put and agreed to.

Clause 140 accordingly ordered to stand part of the Bill.

Clause 141 ordered to stand part of the Bill.

Clause 142

Inquiry into Issues Arising from Data Protection Breaches Committed by or on Behalf of News Publishers

Brendan O’Hara (Argyll and Bute) (SNP): I beg to move amendment 137, in clause 142, page 77, line 34, at end insert—

“(3) The Secretary of State must consult the Scottish Government and obtain its consent before establishing an inquiry under subsection (1).”

This amendment would ensure that before any inquiry was established, the UK Government must have consent from Scottish Government.

The Chair: With this it will be convenient to discuss the following:

Clause 142

Clauses 168 and 169 stand part.

Government amendment 72.

Amendment 138, in clause 207, page 121, line 12, after “subsections” insert “(1A).”

This amendment is a paving amendment for amendment 139.

Amendment 139, in clause 207, page 121, line 13, at end insert—

“(1A) Sections 168 and 169 extend to England and Wales only.”

This amendment would ensure that clauses 168 and 169 would only extend to England and Wales and not apply in Scotland.

Brendan O’Hara: Amendments 137, 138 and 139, which stand in my name and that of my hon. Friend the Member for Cumbernauld, Kilsyth and Kirkintilloch East, were tabled because we believe that the Bill is incompatible with the devolution settlement, trampling roughshod over areas of wholly devolved competence. Whether by accident or design, the Lords amendments
on Leveson—in particular on section 40—that seek to impose a one-size-fits-all Truro to Thurso solution are wholly inappropriate, as they fail to recognise or take cognisance of the fact that in press regulation and criminal justice, to name just two fields, it is the Scottish Parliament, not this place, that has legislative competence. The three amendments draw that distinction and defend the devolution settlement, removing any lingering doubts as to where the hitherto clear legislative boundaries, which have existed since 1998, lie.

Amendment 137 relates to any future inquiry on press standards, styled as Leveson 2. The Scottish National party has been clear throughout that all individuals should be able to seek redress when they feel they have been the victim of press malpractice, and that it benefits each and every one of us to have media that are transparent and accountable. However, we have been equally clear that if there is to be a second part of the Leveson inquiry, the distinct legal context in Scotland must be taken into account. As press regulation and criminal justice are matters for the Scottish Parliament, it is that body that must be consulted about the scale and the scope of any future inquiry and how it will operate in Scotland. As long as the Scottish Government were consulted and the distinct Scottish legal system taken into account, we would be happy to support efforts to establish a second part of a Leveson inquiry because any reasonable person would agree that the terms of reference for that part of the inquiry have not yet been met.

It is unfortunate that we have had to table the amendments. It is not unreasonable to expect the House of Lords to know that press regulation and all the associated issues of the culture, practice and ethics of the press would fall under the devolved competence. A blanket UK-wide amendment would only negatively affect areas of devolved competence. We are disappointed that the amendments were necessary in the first place, but we sincerely hope that Members in all parts of the Committee support our attempts to respect the devolution settlement.

Amendment 139 would ensure that clauses 168 and 169 would extend only to England and Wales and would not apply in Scotland. Again, this is simply a case of our having to tidy up after the Lords. I want to put on record that there is no excuse for what we regard as lazy and entirely inappropriate amendments from the other place. By accident or design, those amendments take no cognisance whatsoever of which powers are devolved and which are reserved. For the future benefit of their lordships, let me say again what I have said on numerous occasions. Although data protection may well be an area of competence reserved to this place, press regulation and criminal justice are wholly devolved to the Scottish Parliament and have been for the past 20 years. If the Bill is not amended, the power of this Parliament will be extended into areas that are solely the preserve of the Scottish Parliament. I believe that will set a very dangerous precedent.

Not only does the Bill drive a coach and horses through the devolution settlement, but I would question why the House of Lords thought it in any way appropriate to apply section 40 of the Crime and Courts Act 2013 to the whole of the United Kingdom, because there is no such piece of legislation as the Crime and Courts Act in Scotland. It simply does not exist. Furthermore, the whole concept of exemplary damages, as I understand is being proposed, is not even recognised and has no equivalent in Scots law. If the Bill were passed unamended, it would force the Scottish Government to pass a legislative consent motion—something they have said they have no intention of doing because, as I said, press regulation and criminal justice are wholly devolved to the Scottish Parliament.

It is simply unacceptable for the UK Parliament to decide what should happen in Scotland with regard to press regulation; that is a job for the Scottish Parliament. The Scottish Government have made it clear that, although they are not opposed to press regulation and are having ongoing discussions with the Scottish media about best to implement an independent press regulation system, it is for Holyrood to decide on a course of action, not to have it decided for them by Westminster. I fully expect the Government to seek to remove clauses 168 and 169 and the Opposition to seek to restore them on Report. I hope that, when the Labour Opposition do that on Report, they will ensure that what they bring back to the Floor of the House of Commons is compatible with the devolution settlement and that the proposed new clause will exclude Scotland from the section 40 legislation.

It is not enough for the Government to say that they understand and sympathise. I urge the Minister to accept our amendments because they preserve and protect the devolution settlement, which has worked well for the past 20 years in terms of press regulation and criminal justice. I ask the Minister and in particular Conservative Members representing Scottish constituencies to respect the devolution settlement and accept that what came back from the House of Lords flies in the face of the long-established devolution settlement. I ask them to accept that it is wholly inappropriate and inconsistent with Scots law and, therefore, support our amendments.

Liam Byrne: I want to say a few words in defence of the clause and touch on the amendments the Government have proposed. The substance of the clause is an attempt to ensure that we activate the second half of the Leveson inquiry, to look into allegations of collusion between the police and members of the fourth estate.

It is worth reminding ourselves of the absolute horror with which we all looked at the revelations about News International’s malpractice. The idea that individuals from national newspapers could hack phones of pretty much anybody in the country, including most notoriously the phone of poor Milly Dowler, sell that information and turn it into front-page newspaper stories, absolutely shocked us. Serious questions were asked about the way the police investigation was conducted. That is why the House united not just to begin the Leveson inquiry, but to propose a second part to look into the question of police collusion. That element was not possible at the time because of the cases that were coming to court, both civil and criminal. The solution proposed by Mr Cameron, the then Prime Minister, which I believe was supported by the present Secretary of State for Digital, Culture, Media and Sport, was that there should be a second half of the Leveson inquiry. Mr Cameron said:

One of the things that the victims have been most concerned about is that part 2 of the investigation should go ahead—because of the concerns about that first police investigation and about
improper relationships between journalists and police officers. It is right that it should go ahead, and that is fully our intention.”— [Official Report, 29 November 2012; Vol. 554, c. 458.]

2.15 pm

Imagine our surprise when the Secretary of State decided to close the Leveson inquiry, saying that the world had changed and that all criminal behaviour and conduct in the fourth estate magically and mystically came to a definitive, categorical and unequivocal end in 2010. That, however, appears not to be the case. Subsequent to the Secretary of State’s declaration that the world had suddenly returned to order and honesty, we heard the revelations of John Ford, a professional blagger employed by The Sunday Times, who set out several detailed allegations and examples of criminal behaviour relating to sensitive information, including on members of the Cabinet and their personal bank accounts. Furthermore, he claims that the practice persists today, saying that “I know individuals who are still engaged in these activities on behalf of newspapers.”

The Secretary of State has no evidential basis for his rather complacent assertion that the practice no longer occurs.

When the Secretary of State presented his decision to the House, most hon. Members who were lucky enough to hear his statement left the Chamber feeling fairly clear that he had explained that Sir Brian Leveson supported his decision to close down Leveson 2. Imagine our surprise when it subsequently emerged that Sir Brian “fundamentally disagrees” with the Government’s decision to end part 2 of the inquiry. Anyone who enjoyed the Secretary of State’s evidence session last week in front of the Select Committee on Digital, Culture, Media and Sport as much as I did will have noticed the rather penetrating questions from my hon. Friend the Member for Wrexham (Ian C. Lucas), which, frankly, the Secretary of State struggled to answer.

When Sir Brian Leveson said that some of the terms of reference could be changed, he was recommending that they be expanded, not restricted, so that the inquiry could look further into how social media companies collect and use data, as well as how they are used as conduits for fake news.

It is probably worth spelling out in more detail some of the evidence that Mr Ford has offered to Parliament. Not all members of the Committee luxuriate in membership of the Digital, Culture, Media and Sport Committee, so they will not all have seen John Ford’s letter of 13 March. It is worth spending some time spelling out exactly what he said, because it is pretty important evidence that touches on Government policy. He states categorically, in black and white:

“I illegally accessed phone accounts, bank accounts, credit cards, and other personal data of public figures (mainly politicians and their families). My targets included politicians of all parties. I was tasked by at least 20 journalists at the Sunday Times, most of them senior, including by very senior executives. They all knew what I was doing and that it was against the law.”

Mr Ford goes on to reflect on the Secretary of State’s response to the urgent question on Wednesday 7 March. The Secretary of State said that the problem with criminal blagging was definitely, unequivocally, categorically a relic of the past and had absolutely, definitely, unequivocally come to an end in 2010. Mr Ford, I am afraid to say, begs to differ.

Mr Ford says in his letter to the Select Committee: “I am sorry to inform you that Mr Hancock is totally wrong”. He goes on to say that “having spent 15 years in the business, it is no surprise...that I still know people in the illegal data theft industry, and specifically...”—this is the nub of the argument—“that I know individuals who are still engaged in these activities on behalf of newspapers.”

So it would seem that there are allegations that the malpractice did not unequivocally, categorically, absolutely, definitely come to an end in 2010.

There is clear evidence before a Select Committee of the House that malpractice continues. The decision therefore to shut down once and for all an inquiry into it can best be described as turning the other way and walking on by. Others, I suspect, will come up with rather fruitier descriptions of what the Secretary of State is up to.

The public policy challenge that the Minister has to reflect on is in the allegations that Mr Ford goes on to make about the inadequacy of the police and the Information Commissioner in taking meaningful action. Mr Ford, I am afraid, is on quite strong ground when he points to a past pattern of behaviour, such as the instance of Steve Whittamore, who was a prolific blagger in the mid-2000s, which neither Operation Glade nor Operation Motorman used to take any enforcement action against newspapers that had paid Whittamore thousands of pounds for illegal blags.

A track record of evidence is, I am afraid, coming to light for action simply not being taken against police officers or newspapers. Mr Ford, regretfully, is drawn to the conclusion that, if we look at the past activities of and the court cases settled by the Trinity Mirror group and News UK, taken together, they show that the police and the Information Commissioner’s Office “are not interested” in or “don’t feel equipped” taking on “newspapers in individual cases”.

I suggest that when we have such extraordinary malpractice, so serious that the result was the closure of one of our oldest national newspapers, and when there is cross-party consensus led not by one of us—by a humble Back Bencher—but by the Prime Minister of this country who made a solemn promise, not only to the House and to Parliament but to the victims of the crimes, that Leveson 2 would go ahead, and we cannot believe those assurances, what are we ever to believe again from the mouth of a Prime Minister? The Minister is shaking confidence in prime ministerial pronouncements and in the cleanliness and hygiene of the fourth estate. One simply has to ask, what on earth are they worried about that would surface in Leveson 2?

The Secretary of State tried to rest his arguments in the House and before the Select Committee on the idea that many of the allegations that Mr Ford made had been reviewed comprehensively in Leveson part 1, but that completely ignores the solemn promise made by the Prime Minister of this country that Leveson 2
would take place. It also ignores the crucial evidence in Mr Ford’s statement that he says that he knows of illegal activity that still persists. The Minister will probably say, “Well, if that’s the case, it’s a crime and should be reported to the police,” and so on, but what we learned during Leveson 1 is that case studies such as that tend to be tips of icebergs. The real worry is that the iceberg in this case is wholesale police and newspaper collusion that, frankly, should be weeded out.

Over the past three or four years, we have learned to our great cost of the need sometimes to delve deep into the past—into the track record of offences, whether that is Hillsborough, Orgreave or the evidence surfaced by Leveson 1—to get to the truth so that public policy and reform can be better in the years to come. I do not understand why we would not take a systemic look at the allegations of collusion between the police and the media to satisfy ourselves that the system is beyond improvement.

I want to finish with the words of Madeleine McCann’s father, Gerry McCann, whose family was unfortunately libelled and intruded upon by the press following Madeleine’s disappearance. When he learned that the Government are scrapping Leveson part 2, he said that “this Government has abandoned its commitments to the victims of press abuse to satisfy the corporate interests of the large newspaper groups...This Government has lost all integrity when it comes to policy affecting the press.”

I hope that, having reflected on those harsh and serious words, the Minister will conclude that we have nothing to fear, nothing to hide and everything to gain from letting Sir Brian Leveson finish the job the Prime Minister said he would be allowed to finish.

Peter Heaton-Jones (North Devon) (Con): It is a pleasure to serve under your chairmanship, Mr Streeter. I declare an interest: I was a journalist for many years—I am no longer practising—although not in the hard-copy newspaper industry. Given my background, I take a deep interest in these matters.

I have a great deal of sympathy for the reasons for the Scottish National party tabling amendments 137, 138 and 139, and I absolutely understand the need for the tidying up that needs to be done to the amendment that has come from the other place, which appears to be added in relation to the legal situation with the Scottish Parliament’s devolved powers. I fully understand why the Scottish amendments have been tabled, and I have sympathy with the view that the Lords amendment needs tidying up. However, I cannot support the SNP amendments simply because I do not want the amendment from the other place, to which they would be attached, to be part of the Bill at all. I will go through some reasons to explain why, but I want to put on the record my sympathy for the reason for them being tabled.

The hon. Member for Argyll and Bute described the amendment from the other place as “lazy” because it does not take into account the Scottish devolved powers. That is one description of it. It is also, frankly, a bit mysterious. I find it a little hard to understand why we are discussing this issue at all in relation to the Bill. That amendment and the section 40 amendment, which we will discuss later, were attached to the Bill in the other place in much the same way as one attaches decorations to a Christmas tree. They are not part of what we should be discussing, although I am grateful that we have the opportunity so to do, because that allows the Government to put their case, as I am sure Ministers will do shortly, and as my right hon. Friend the Secretary of State did in the House earlier.

As I set out in my speech on Second Reading, I believe strongly that we should reject the amendments that have come to us from the other place—in particular, the amendment relating to Leveson 2. I heard everything the right hon. Member for Birmingham, Hodge Hill said about the need for Leveson 2 and about victims needing their day in court. I am not putting words into his mouth—I do not think he used exactly that phrase, and I do not disagree—and there is indeed a difficulty in that, of course, there are still examples of reporters working for a variety of news organisations who are undertaking practices that are either immoral or illegal, or in some cases both.

2.30 pm

When I started work as a journalist in 1986, it was quite clear that that was going on, and it is quite clear to me now that that is still going on. Establishing Leveson 2 would not change that; it would not put it right; it would not solve any of those wrongs. It would not even bring the sort of justice that I am sure we all want for members of the public who have been wronged by the media.

The right hon. Gentleman made great play on the fact the former Prime Minister said that Leveson 2 will go ahead. Indeed, he did. It was before my time in the House—I am not as long serving as other Members—but the fact is that things have changed markedly since the former Prime Minister made that commitment on going ahead with Leveson 2. The landscape has changed markedly. It is absolutely right that we take account now, in 2018, of the situation that we find ourselves in. Given that Leveson 1 has happened, given what we know Leveson 1 was able to achieve and what it was not able to achieve, and given some of the reforms that have since taken place, it is absolutely right that the current Government in 2018 revisit the matter. In my view, they have reached absolutely the correct conclusion: the grounds on which Leveson was originally to go ahead no longer are justified.

Liam Byrne: Like the hon. Gentleman, I wish that the entire media operated with the editorial standards of BBC Essex and the Swindon Advertiser. I was struck by a remarkable statement: that he believes that the mispractice or malpractice still goes on—I have written down carefully the words that he used. I cannot, therefore, understand why the conclusion he draws from the persistence of malpractice is to look the other way and to shut down an inquiry into whether it took place and who the guilty are. I would be grateful if he can correct me on my misunderstanding.

The Chair: Order. First, let me correct a possible misunderstanding. The right hon. Member for Birmingham, Hodge Hill mentioned that clauses 168 and 169 will be debated later. In fact, we are debating them as part of this group, as I tried to make clear when I introduced amendment 137.

Peter Heaton-Jones: Thank you for that clarification, Mr Streeter.
There is nothing remarkable about what I said. Quite clearly, there is still malpractice going on in the journalism industry. Is the right hon. Gentleman honestly trying to say that is a remarkable thing to say?

Liam Byrne: Yes.

Peter Heaton-Jones: It is not remarkable at all. Of course it is going on, but establishing and carrying out Leveson 2 would do nothing to solve that problem and nothing to bring justice to the members of the public who have been done wrong by that small number of journalists who are acting in that way. I do not know why the right hon. Gentleman finds that a remarkable statement to make.

As for the statement that he made on Second Reading—that the Government’s position is to say, “Nothing to see here—absolutely nothing happening”—that is not what the Government are saying at all. The Government’s position is clear: Leveson 2 simply would not do what I think the right hon. Gentleman and probably everyone in this room would like it to do, which is to be some sort of cleansing disinfectant that solves all the problems. It simply will not do that.

Liam Byrne: As much as I respect the hon. Gentleman’s omniscience, how could he possibly know that?

Peter Heaton-Jones: It is a big gamble to spend potentially £50 million when we are not sure whether it will have the required outcome. That is the point. The Lords amendment would start the Leveson 2 process, which would cost at a very conservative estimate £50 million, potentially last for a huge amount of time and still not get to the answer that we want. There must be better solutions.

I had started to discuss the fact that the landscape has changed and that the very framework in which we work has changed markedly since the former Prime Minister made the commitment to go ahead with Leveson 2. There have been huge changes. Not only have we had the Leveson 1 inquiry, which in its own terms of reference touched on many of the issues that the proposed Leveson 2 inquiry would cover, but we have had any number of changes, improvements, and reforms in the way the police and indeed the media operate. We have had Operations Elveden, Tuleta and Weeting, which included Operation Golding, all of which have investigated a wide range of practices in the interaction between the police and members of the media and journalists. At a total cost, incidentally, of about £40 million for those operations, they have done good work and all of them have resulted in significant reform.

When I first joined the journalistic trade, way back in 1986, there was malpractice on a scale that we would not believe, and it was completely normal for journalists to pick up the phone to a friendly police contact and get whatever information they wanted to write their next report. That was absolutely normal. It is not normal now. I am sure it still happens, but it is now not the norm, which is good. That is why we do not want to turn the clock back and commit ourselves to a very long inquiry—a Leveson 2 inquiry—which would not do what we want it to do.

Where malpractice occurs in the media, where cases such as those raised by the right hon. Gentleman come to light, and where members of the public are treated in the most despicable way by journalists, I want people to be able to have the right to redress, to have their day in court, and to be able to say, “This is what has happened and it must change,” but Leveson 2 would not do that. It would not provide the means by which that happened. That is why the Secretary of State for Digital, Culture, Media and Sport was absolutely right to make the decision and to say that Leveson 2 is not on the Government’s agenda, and nor should it go ahead. It is perhaps worth pointing out also that this Government were elected only nine months ago on a manifesto that specifically said that Leveson 2 would not go ahead. That was a manifesto commitment.

Mr Streeter, may I just seek absolute clarification from you? From your earlier instruction, are we now also talking about section 40?


Peter Heaton-Jones: Yes it does. May I go on to address that briefly as well at this point, if that is in order?

The Chair: I would be delighted if the hon. Gentleman did that.

Peter Heaton-Jones: Thank you very much indeed.

I do not really have much to say. To be clear, we are considering the amendment made in the other place. It seeks to enact section 40 of the Crime and Courts Act 2013, which this Government and the Secretary of State have said we will not do—indeed, they have said that we wish to repeal section 40.

It is very clear in my mind that we need to reject the amendment made in the other place. There is a very straightforward reason, which is that section 40 does one key thing: it seeks to persuade media organisations, specifically newspapers, that have not signed up to a recognised regulatory body to do so by providing a financial inducement of the most “blunt instrument” kind.

I have here a document from the House of Commons Library; for the record, I emphasise that the House of Commons Library is neutral. The document discusses why section 40 of the Crime and Courts Act 2013 was introduced. The Library says that it was intended to “coerce or incentivise publishers to become members of a recognised regulator”.

That is language that we should be worried about. The reason we should be more worried about what section 40 will do—it is pretty straightforward—is that if a member of the public brings a defamation action against a newspaper, it goes to court and the newspaper wins the case, that media organisation is still financially liable to pay the costs of both sides.

Quite simply, that will encourage a lot of entirely superfluous and vexatious legal actions to be brought by people who just have some kind of beef against the media and pockets bulging with cash that allows them to do so. When, as will inevitably happen, the media
wins the case, because it was built on sand, the media organisations concerned will be put out of business by the requirement to pay the legal costs on both sides.

**Liam Byrne:** The Minister is cheering on the hon. Member, but will he for complete clarity remind the Committee who proposed this architecture in the first place? From memory, it was his right hon. Friends the Members for West Dorset (Sir Oliver Letwin) and for Basingstoke (Mrs Miller).

**Peter Heaton-Jones:** I was not in Parliament at the time. I have only been here for two and a half years. We go back to the point that I made in relation to the previous clause. The ground has shifted. We now know what the effect will be. The other place debated this in some detail; the arguments were put extremely strongly, and by a narrow majority their lordships, as is their right, passed the amendment and asked us to consider it. It is perfectly right that they are asking us to consider it. It is perfectly right that we say: “Up with this we will not put.” Section 40 will have precisely the opposite effect to what probably anyone listening would hope it have. It will be an extraordinarily damaging measure for the future of the freedom of the press in this country. It will have the effect of preventing publication of material which is in the public interest and which is true, legitimate, and fair, because newspaper proprietors will not be able to afford the risk of going to a court case which they win but still have to pay the costs. It will be an incredible impediment to the free press in this country. For that reason more than any other we must reject the amendments that come from the other place.

**The Chair:** One or two colleagues have caught my eye because I was not clear enough in my introduction to this section. I invite Mr Liam Byrne to readdress the Committee in relation to these clauses.

**Liam Byrne:** I am grateful to you, Mr Streeter, for setting that out so clearly. I want to speak in defence of clauses 167 and 168.

I am clearly an innocent abroad in a world that is not innocent. I struggle to follow the argument made by the hon. Member for North Devon. On the one hand he was pretty insistent that malpractice continued, but then invited us to believe that somehow the world had changed comprehensively. Either the world has changed or it has not. I fear that the world has changed a bit, but not enough, so there is still a need for an effective means of offering justice to those who have been maligned by newspapers.

The architecture set up by the right honourable Members for West Dorset and for Basingstoke was complicated. We have a fine tradition of a free press, going back to Sir Brian Leveson’s recommendation that there be some kind of low-cost, readily accessible form of arbitration and settlement when the press, so help them, get things wrong. People make mistakes; to err is human, so we have to ensure that human institutions have a means of fixing things when mistakes are made. Many of the victims who suffer at the hands of the press may be poor people, not rich people, who do not have access to expensive lawyers who can file emergency injunctions to stop publication overnight, as we know many celebrities have.

The challenge that confronted the previous Prime Minister and the right hon. Members for West Dorset and for Basingstoke was how to ensure that we sustain a free press, which is so important to the culture of free speech in this country, and deliver justice to those who have been maligned—how to ensure that justice is accessible to them. The proposal that was constructed was fairly elegant. It sought to ensure two things: first, that there was an independent code of practice and secondly, that there a low-cost form of arbitration. As it happens, the only regulator that has come forward with those mechanisms and been recognised is IMPRESS.

**IMPRESS** is bedevilled by well-known problems, but the only current alternative is the Independent Press Standards Organisation. The challenge with IPSO is that it is not independent and it operates a code based on the old editors’ code, which is subject to changes on a whim. Although it has just about put in place a low-cost arbitration scheme, it has never been tested in anger, so we do not know whether it will work.

Conscious of that, the previous Prime Minister decided that the best way to balance the difficult things that we needed to balance and to make progress was to accept Sir Brian Leveson’s recommendation that there be some sort of fiscal incentive for people to do the right thing and create a regulator that does the business for justice for people who are maligned by the press. That is why the architecture was constructed in that way.

In 14 years, I have never heard of such a comprehensive volte-face by a Government as casting away a policy of which they were the architects. They were the architects of the policy. They worked hard to get cross-party consensus. They made promises to the victims of press injustice that the policy would be carried through. Now, the Conservative party decides to put all those promises, those policies and that delicate balance in the bin. That is unwise. The British public have some right to, not perfect consistency, but a degree of consistency from a governing party.

We have heard that the world has not changed, and we have heard that there was a history of police collusion with newspapers. I do not think that turning a blind eye is the way to remedy historic injustice or to perfect public policy for the years to come. The British public deserve a degree of consistency in the delivery of the scheme that the previous Prime Minister set out with all his customary eloquence just a couple of years ago. That is why these amendments are important. They will be rebutted on Report if the Government succeed in defeating them here.

I accept the arguments made by the hon. Member for Argyll and Bute about the need to perfect the amendment, but the problem is not going away. If the hon. Member
for North Devon is right, there are many further landmines along the road. Having worked with the police over the last 14 years in my role as a constituency MP, the one thing I know about police officers is that they hate bad apples, so they are frustrated when bad apples are allowed to continue in the organisation. We should be casting those individuals out root and branch.

We should also reflect on past misdemeanours to satisfy ourselves that we have good systems, good policy and good laws in place to guard against that kind of malpractice in the future. That is how we improve the country: by reflecting on past mistakes and making corrections. Turning a blind eye never, ever works. That is how we improve the country.

Matt Warman (Boston and Skegness) (Con): I shall be mercifully brief. As a print journalist for 15 years, I start by saying that the entire industry was genuinely horrified to learn of the extent and the offences that had been committed by organisations that, in the main and over many centuries, worked genuinely in the public interest. We should not forget that journalists who work in the media today, and were doing so while that was going on, are in the main trying to do the kind of public service that we would all defend. We should not underestimate the horror with which the industry greeted the stories of what happened to the Dowler family and many others, be they celebrities or other victims. I hope we would agree across the House that the media in the main have fulfilled that remit. I should also say, as did my hon. Friend the Member for North Devon, that I have a great deal of sympathy with the amendments proposed by the Scottish National party. We should prize consistency above all else in this area.

The right hon. Member for Birmingham, Hodge Hill said that he was surprised to learn that the Government did not seek to proceed with the second part of the Leveson inquiry. It was in our manifesto, so his surprise is surprising. I can only conclude that he did not read the Conservative manifesto. Perhaps he read the Labour manifesto and was so horrified he could not face reading another one.

Liam Byrne: I just could not understand it.

Matt Warman: The Labour one? Quite right. We should bear in mind the two things used in favour of the position taken by the Conservative party and the Government in the manifesto. The first, as my hon. Friend the Member for North Devon said, is that the world has indisputably moved on. The challenges that face our modern media are not the challenges that would have been subject to the Leveson inquiry. The more important point is that, where there are legitimate concerns about the media and how people are treated, the solution to that is effective and independent regulation, and that is what we have now more than ever.

Liam Byrne: The hon. Gentleman served on The Daily Telegraph long enough to know that the IPSO code today bears a striking resemblance to the old editors’ code. Perhaps he could give us the benefit of his experience and tell us whether he is satisfied that the IPSO code meets the tests set out by Sir Brian Leveson and agreed in all parts of the House.

Matt Warman: I will say two things. I had a mercifully limited engagement with what was then the Press Complaints Commission, although we did have to deal with some complaints in my small bit of the paper. Although we took it seriously, it is in no way comparable with the seriousness that IPSO is now taken. That might be down to the fact that the scale of the apology that can be demanded by IPSO, and has to be given, is exponentially greater. That is a crucial deterrent when it comes to the work done by journalists in the newsroom, who sometimes regard their editors as figures of great fear as much as great role models.

The other side is that we have a crucial low-cost arbitration system that allows people who are not of the means that the right hon. Gentleman described to bring cases against the media and get the redress they deserve when people make mistakes. Those are the two crucial differences between the PCC and IPSO. The latter is a fundamentally more powerful, very different regulator, but it has the credibility and independence that IMPRESS will simply never have.

Liam Byrne: Would the hon. Gentleman give way?

Matt Warman: I thought the right hon. Gentleman might want to come in.

Liam Byrne: The hon. Gentleman was an experienced and respected journalist and has a track record on which to draw in his reflections. He did not quite answer the question whether he thought the code of conduct that IPSO regulates meets the tests set out by Sir Brian Leveson and agreed on both sides of the House. Will he reflect on whether the code of conduct is prone to changes driven through by newspaper editors? There is no guarantee that newspaper editors cannot influence that code, and its shape and bite, in the years to come.

Matt Warman: The right hon. Gentleman is right that there is a continuous thread to the sensible key principles of press regulation, and for journalists to have a role in shaping those is not entirely illegitimate. None the less, we must bear in mind that those principles should serve the public before they serve the press. That is what is in the principles that Sir Brian Leveson sought to suggest. The right hon. Gentleman is right that we agree on those on both sides of the House, and that IPSO strikes the right balance. The sense that both the world and the regulator have changed should reassure both Opposition Members and members of the public who would like the Government to secure a free but sensibly regulated press that serves all of us.

Colin Clark (Gordon) (Con): Surely my hon. Friend makes great play of David Cameron promising IPSO, but I would make great play of Government
delivering on the manifesto pledges they made when they fought an election in 2017. Not doing what he set out also delivers on a promise—the more recent promise should take precedence.

My hon. Friend the Member for North Devon powerfully made the case against section 40, which seeks to punish the victim. That would obviously have a clear chilling effect not only on our local newspapers, which are often on the brink of bankruptcy, but on the broader media.

We can look at fantastic pieces of journalism even today, such as the one about Cambridge Analytica. The Guardian itself says, “Please, we would like your donations so we can keep our valuable journalism free”—the paper has had to fight off three pieces of legal action by Cambridge Analytica and one from Facebook. Those huge corporations seek to shut down legitimate investigation, and the right hon. Member for Birmingham, Hodge Hill suggests that if they were to bring and win cases, The Guardian should pay for them. That is an extraordinary position to take.

Liam Byrne rose—

Matt Warman: I am sure the right hon. Gentleman is about to assure me that he is not taking that position.

Liam Byrne: Let us be real about this. The idea that companies such as Facebook or Cambridge Analytica will desist from legal action to shut down stories that they do not like—the idea that that will not happen at any time in the future, even under the existing regimes—is for the birds. The argument that is better made by some of the hon. Gentleman’s colleagues is to do with the risk to local newspapers, most of which are now owned by Trinity Mirror, which makes tens of millions of pounds in profit, or the Johnston Press. The point is that vexatious claims can be shut down and thrown out at any one of three stages by the regulator or, before the case goes to arbitration, by the arbitrator or by a judge, so the incidence of costs arising will not be on the scale the hon. Gentleman anticipates. Equally, he must accept that, without a form of low-cost arbitration, justice is denied to people who are maligned by newspapers.

Matt Warman: I enjoyed the right hon. Gentleman’s speech, but I disagree with him profoundly. I worked for a newspaper that had, by comparison with our local papers, an enormous budget. The threat of their piece of work costing their newspaper and their boss tens of thousands of pounds, they simply would not get hired, never mind allowed into print.

3 pm

Liam Byrne: Finally and very briefly, the hon. Gentleman is making an eloquent argument. Why, then, was that proposed by the right hon. Members for West Dorset and for Basingstoke? How did they get it so profoundly wrong?

Matt Warman: That is a fascinating philosophical question, but I can only tell the right hon. Gentleman that I would not have voted for it. I appreciate that he will say that it is easy for me to say that now, but the idea that people in this place would be convinced that it is the best possible model is simply not plausible after the statements that my hon. Friend the Member for North Devon and I have made today. Surely we need a set of press regulations that preserves the independence of the media, and their ability to invest in journalism at local and national level, which we all want if we are to hold the powerful to account. We also need regulations that allow hon. Members to say with a clear conscience that we have done nothing that puts those businesses in serious jeopardy.

It does not seem to me that a costly Leveson 2 is the best use of public money, or that the threat of section 40 will ever be the best use of private money, putting legitimate local and national media out of business. Those arguments seem to me like a powerful case for IPSO, and for a sensible look at the sustainability of the press, as the Prime Minister has set about doing. They do not under any circumstances seem to me like a good reason to vote for the amendments.

Margot James: I will set out the Government’s position on clauses 142, 168, 169 and 205, before returning to the amendments in the name of the hon. Member for Argyll and Bute.

As we have heard, clause 142 requires the Government to establish an inquiry with terms of reference similar to those contained in part 2 of the Leveson inquiry, but in relation to data protection only. The Government set out our intention not to reopen the Leveson inquiry in our response to the consultation on the future of the inquiry on 1 March. I will not repeat the arguments in full, but I will say that the Government’s firm focus is on the problems faced by the media right now.

The Government recognise that there is a great deal of feeling on both sides of the debate. We have listened to all views, including those of victims, in reaching a decision. No one seeks to excuse the past behaviour of individual media organisations, nor to legitimise it. As the right hon. Member for Birmingham, Hodge Hill said, some of the stories we heard at the beginning of the Leveson inquiry were horrific. The Government have a duty, however, to make decisions that are proportionate and in the public interest. In the light of all the evidence available, it is apparent that part 2 of the inquiry is no longer appropriate or proportionate.

Part 1 of the inquiry lasted over a year, and heard evidence from more than 300 people, including journalists, editors and victims. Since then, the majority of the Leveson recommendations have been implemented. Three
major police investigations examining a wide range of offences have been completed. More than 40 people were convicted, some of whom were sent to prison. There have also been extensive reforms to policing practices, and significant changes to press self-regulation.

As a result, the terms of reference for part 2 have largely been met, and the culture that allowed phone hacking to become the norm has changed. Meanwhile, the media are facing critical challenges that threaten their sustainability, including fake news, declining circulations and gaining revenue from online content. Free and vibrant media are vital to democratic discourse, and we need to tackle those challenges urgently. Holding a costly and time-consuming public inquiry looking predominantly backwards is not the right way to go.

The Government are committed to addressing these issues, and we are developing a digital charter to ensure that new technologies work for the benefit of everyone, with rules and protections in place to keep people safe online and to ensure that personal information is used appropriately. As part of that, we are also undertaking work to ensure that there are sustainable business models for high-quality media online. The media landscape is different and the threats are different, too. Issues such as fake news mean there is a need to protect the reliability and objectivity of information.

Likewise, clauses 168 and 169 are similar to the provisions contained in sections 40 and 42 of the Crime and Courts Act 2013, but apply to breaches of data protection law only. The Government do not believe that introducing a provision similar to section 40 of the 2013 Act into the Bill is appropriate, but in relation to data protection only. That is particularly so given our decision earlier this month to repeal section 40 when there is a suitable legislative vehicle. In coming to that decision, we considered all the available evidence, including the views of respondents to the public consultation that we undertook last year. Many respondents cited concerns about the chilling effect that section 40 would have on the freedom of the press, which was so ably summed up by my hon. Friend the Member for Boston and Skegness.

Liam Byrne: Will the Minister tell the Committee why she supported it when it came to a vote last time?

Margot James: The right hon. Gentleman has made great play of the former Prime Minister’s statement. I remind him that that statement was given six years ago. Much has changed since. My hon. Friend the Member for North Devon tried to make the point that, although we cannot rule out that egregious conduct is still going on in the press, as I imagine there is in virtually every other sector of society, we can agree that much has changed and improved. That is why the Government have changed their direction. I hope that satisfies the right hon. Gentleman.

Gareth Snell (Stoke-on-Trent Central) (Lab/Co-op): It is a pleasure to serve under your chairmanship, Mr Streeter.

On that point, the Minister accepts that egregious activity could be taking place across the industry but does not think that the proposal is the appropriate vehicle for dealing with it. She believes that the digital charter is the appropriate vehicle, but what evidence is she using to ensure that that addresses the egregious activity?

Margot James: I want to correct one thing that the hon. Gentleman said: I did not say that that activity was taking place across the industry; I said that it was still taking place. Indeed, we have heard the horrendous allegations made by John Ford, albeit referring to behaviour that predates 2011. He alleges that it is still going on. I am not denying that it probably is still carrying on in pockets, but I would not say that it is widespread.

Press self-regulation has changed significantly in recent years with the establishment of IPSO, which follows many of the principles set out in the Leveson report. As so few publishers have joined a regulator recognised under the royal charter, commencement of section 40 would have a chilling effect on investigative journalism, which is so important to a well-functioning democracy.

Daniel Zeichner (Cambridge) (Lab): It is a pleasure to serve under your chairmanship, Mr Streeter. We keep hearing about the chilling effect—it is well rehearsed—but could the Minister confirm that it could be entirely avoided if newspapers sign up to an appropriate regulator, which does not have to be IMPRESS? It is not a difficult thing to do.

Margot James: Currently, IMPRESS is the only regulator recognised under the royal charter. I cannot speak for the press. There was a heated debate when the legislation went through Parliament. The press decided as one not to join what they perceived as a state-backed regulator. IPSO now does the job, albeit the Financial Times and The Guardian alone among the broadsheets have not joined IPSO.

The media landscape has changed. As I noted earlier, high-quality journalism is under threat from the rise of clickbait and fake news, from difficulties in generating revenue online to replace the revenue that used to flow from printed sources, and from the dramatic, continued rise of largely unregulated social media. If implemented, section 40 could impose further financial burdens on publishers, particularly at local level—200 local papers have closed in the last decade.

On top of that, the amendments made in the other place undermine our Scotland and Northern Ireland devolution settlements—that point was ably made by the hon. Member for Argyll and Bute. The proposed new clauses seek to legislate on a UK-wide basis despite press regulation being a reserved matter for the devolved Administrations, which brings me to amendments 137, 138 and 139 in the name of the hon. Gentleman.

The Government are sympathetic to the hon. Gentleman’s arguments for reasons I have set out. We will nevertheless push instead for the removal of those clauses from the Bill in their entirety. Similarly, while we agree with the sentiment of amendment 137, which seeks to require the Government to obtain the Scottish Government’s consent before establishing an inquiry under clause 142, we note that there is already a consultation requirement to that effect in the Inquiries Act 2005. Such an amendment is therefore unnecessary.

To conclude, high-quality news provision is vital to our society and democracy. I know there is shared interest across the House in safeguarding its future, and the Government are passionate about and working to
deliver it. We believe that the clauses would work against those aims and cut across the work we are doing to help strengthen the future of high-quality journalism, and will therefore oppose their continued inclusion in the Bill.

Brendan O'Hara: I take on board what the Government say and appreciate that they have accepted the principle of the amendment, but I still intend to push it to the vote. It is essential that the devolution settlement is protected in as broad and deep a way as possible. I understand that they would seek to remove the entire clause, but if the clause is passed and de-amended, it has serious consequences for the devolution settlement. For that reason we will be pushing it to the vote.

Question put, That the amendment be made.

The Committee divided: Ayes 9, Noes 10.

Division No. 10]

AYES

Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren
McDonald, Stuart C.

Murray, Ian
O’Hara, Brendan
Snell, Gareth
Zeichner, Daniel

NOES

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

Jack, Mr Alister
James, Margot
Lopez, Julia
Warman, Matt
Wood, Mike

Question accordingly negatived.

Question put, That the clause stand part of the Bill.

The Committee divided: Ayes 9, Noes 10.

Division No. 11]

AYES

Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren
McDonald, Stuart C.

Murray, Ian
O’Hara, Brendan
Snell, Gareth
Zeichner, Daniel

NOES

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

Jack, Mr Alister
James, Margot
Lopez, Julia
Warman, Matt
Wood, Mike

Question accordingly negatived.

Clause 142 disagreed to.

Clause 143

INFORMATION NOTICES

3.15 pm

Margot James: I beg to move amendment 51, in clause 143, page 77, line 37, after “notice”)” insert “—

(a) ”.

See the explanatory statement for Amendment 52.

The Chair: With this it will be convenient to discuss Government amendments 52, 54, 126 and 58.

Margot James: The Information Commissioner has a breadth of corrective powers at her disposal to investigate breaches of data protection legislation. One such power is the ability to issue an information notice on a data controller requesting that they provide the commissioner with specified information. Article 2 of the general data protection regulation states that certain types of processing of personal data, including purely personal or household activities, are exempt from the provisions of the GDPR. That includes the list of all those hon. Members who deserve a Christmas card this year.

Although such processing is exempt, it is important that in certain situations the Information Commissioner is able to verify that the processing actually meets this test and does not fly under the radar of GDPR requirements unduly. Government amendments 51 and 52 will ensure that the Information Commissioner is able to issue an information notice, in order to determine whether the process is genuinely being undertaken in the course of a purely personal or household activity.

Government amendment 54 is a consequential amendment. It ensures that the reference to processing of personal data in the subsection added by Government amendment 52 means any type of processing, pulling on the definitions provided in subsections (2) and (4) of clause 3, rather than those under parts 2, 3 or 4, none of which apply to processing in the course of purely personal or household activities.

Government amendments 58 and 126 make further consequential changes to clause 159 and paragraph 9 of schedule 16. The amendments ensure that certain safeguards for controllers and processors in the context of enforcement action extend to all persons, since their exact status may in fact be the source of dispute.

All in all, this a common sense set of changes that enjoy the full support of the Information Commissioner’s Office.

Amendment 51 agreed to.

Amendments made: 52, in clause 143, page 77, line 40, at end insert “,” or

(b) require any person to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of determining whether the processing of personal data is carried out by an individual in the course of a purely personal or household activity.”

This amendment and Amendments 51 and 54 enable the Information Commissioner to obtain information in order to work out whether processing is carried out in the course of purely personal or household activities. Such processing is not subject to the GDPR or the applied GDPR (see Article 2(2)(c) of the GDPR and Clause 21(3)).

Amendment 53, in clause 143, page 78, line 23, leave out “with the day on which” and insert “when”.

This amendment is consequential on Amendment 71.

Amendment 54, in clause 143, page 78, line 30, at end insert—

“(10) Section 3(14)(b) does not apply to the reference to the processing of personal data in subsection (1)(b).”—(Margot James.)

This amendment secures that the reference to “processing” in the new paragraph (b) inserted by Amendment 52 includes all types of processing of personal data. It disapplies Clause 3(14)(b), which
Louise Haigh: In this of all weeks, it is particularly relevant that we debate this clause, which relates to information notices, and the powers and enforcement sanctions available to the Information Commissioner, given the horrendous breaches of our data regulation that have been exposed by Channel 4 and The Guardian.

The Secretary of State for Digital, Culture, Media and Sport told the House yesterday that the Information Commissioner was seeking further powers to compel compliance with information notices, testimony from other individuals in complex investigations, such as that into Cambridge Analytica, and criminal sanctions for breaches of information notices.

Under the current data protection legislation, breach of information notice is a criminal offence that carries a custodial sentence. The maximum sentence under this Bill is only a fine. That is a significant weakening of the data protection regime and its sanctions. Indeed, in her own evidence, the Information Commissioner said:

“The new approach in the Bill of failure to comply with an” information notice

“no longer being a criminal offence but punishable by a monetary penalty issued by the ICO is likely to be less of a deterrent, as data controllers with deep pockets might be inclined to pay the fine, rather than disclose the information being requested.”

I would be grateful if the Minister could set out exactly why the Government have decided to weaken the powers given to the Information Commissioner and the sanctions available to her.

Crucially, the Information Commissioner has requested the power to compel compliance with information notices. As things stand, it is an offence not to deliver information, but the Information Commissioner does not have the power to demand compliance with information notices. She has said that that puts us out of step with our closest EU member state neighbour, Ireland, which has a much stronger data protection regime, with much tougher sanctions and, indeed, powers to compel compliance with an information notice.

That gap in the Information Commissioner’s enforcement powers has not caused significant problems up to now, because formal action has largely centred on security breaches or contraventions of the privacy and electronic communications regulations. In such cases, the commissioner rarely needs to use her information notice powers, because the evidence of a contravention is usually clear and in the public domain.

Where the Information Commissioner has used her enforcement powers against a data controller for contraventions of the data protection principles under the Data Protection Act, she has generally found data controllers to be co-operative because, under the current framework, financial penalties are reserved only for the most serious contraventions of the law. However, as investigations become more complex—and as we are seeing this week—the Commissioner will be unable to obtain the information she needs.

The Minister has said that the Government are considering potential amendments to the Bill, as laid out by the Secretary of State yesterday. It is baffling, however, that those amendments have not already been tabled, given that the Information Commissioner suggested them in her written evidence earlier in the process. The provisions represent a serious weakening of the existing regime and a failure of the Government to step up to the plate on the matter of the complex investigations conducted by the Information Commissioner.

Margot James: I do not accept that this Bill represents a reduction in the powers of the Information Commissioner, and I do not think that that is her view either. Obviously, I accept what she said in response to questioning from Select Committee on Digital, Culture, Media and Sport. As I have already said, my right hon. Friend the Secretary of State is considering her request, and we are working on the areas where she feels there is a shortfall.

I reassure the Committee that the Bill strengthens ICO’s overall powers. The hon. Member for Sheffield, Heeley has mentioned fines. There are fines of up to 4% of global turnover, or £17 million, both for malpractice itself and for blocking investigations and inquiries mounted by the ICO.

Liam Byrne: One way in which the Government could row in behind a frustrated Information Commission would be to deny Government contracts to companies that are behaving badly. I understand that Cambridge Analytica has Government contracts with both the Foreign Office and the Ministry of Defence. Are they under review?

Margot James: I cannot speak for either of those Departments. We are debating the powers of the ICO rather than contractual matters between private companies and Government Departments. I accept that that is a moot point, but it is not the purpose of this Bill Committee to go into those details.

To return to the points raised by the hon. Member for Sheffield, Heeley, we are strengthening the powers of the Commissioner. We are extending her current power to serve assessment notices on data controllers in public sector bodies to all data controllers across the private sector as well. Those assessment notices will require them to provide evidence of their compliance with the law, and there is now the power to enforce assessment notices by obtaining a warrant to exercise search and seizure powers on behalf of the ICO. The Bill also creates a criminal offence for obstructing a warrant, which is subject to both fines and a criminal record. We are strengthening in those areas and also increasing fines substantially.

Liam Byrne: I understand that the Minister cannot answer the detailed question about Government contracts with, for example, Cambridge Analytica, but does she think, philosophically, that a Government would and should reconsider contracts with companies that are not complying with a reasonable request made by the Information Commissioner?

Margot James: The right hon. Gentleman makes an entirely reasonable point. As I said earlier, I cannot go into it in a debate on this particular Bill, other than to say that he makes a reasonable point.
Clause 143 provides the commissioner with the power to issue an information notice. This is a type of notice that requires a controller or processor to provide the commissioner with specified information within a certain time period.

*Question put and agreed to.*

Clause 143, as amended, accordingly ordered to stand part of the Bill.

Clause 144 ordered to stand part of the Bill.

**Clause 145**

**FALSE STATEMENTS MADE IN RESPONSE TO AN INFORMATION NOTICE**

*Question proposed,* That the clause stand part of the Bill.

**Liam Byrne:** The operation of clause 145 is a matter of great public concern this week, because of the revelations that an app that sat on Facebook collected data for a particular purpose, but they were then re-used by Cambridge Analytica for an entirely different purpose, to bend the outcome of particular elections and, quite possibly, referendums too. Facebook had made a statement that the matter had been resolved a couple of years ago and that the relevant data in question had been deleted. The story has developed over the past 24 hours and former Facebook employees are now alleging that it was not simply 50 million records that were collected for one purpose and re-used for another; there may have been hundreds of millions of records collected for one purpose and used for another.

How will clause 145 bite on a company such as Facebook that may be responding to an information notice issued by the Information Commissioner? The company may have told the Information Commissioner that it was all fine, the data was all deleted and everyone was perfectly satisfied, but a couple of years later it transpires that that is not the case. What would then happen to a company such as Facebook? Is the Minister satisfied that the proposed sanctions and penalties are strong enough? It is not clear to me, given what we now know, that these sanctions are strong enough at all.

**Margot James:** We are debating a suite of powers as part of the overall powers with which the Bill reinforces the Information Commissioner’s Office. It is not just about clause 145. If a company discloses information unlawfully, there is also a separate offence in clause 170. We are not relying on one clause alone.

3.30 pm

The case to which the right hon. Member for Birmingham, Hodge Hill is referring is developing and ongoing as we debate the Bill, but the Information Commissioner is investigating whether the Facebook data that he referred to was illegally acquired and used. The investigation will focus on establishing what information was accessed and what measures were in place to protect that information, if any, in relation to Facebook users in the UK.

*Question put and agreed to.*

Clause 145 accordingly ordered to stand part of the Bill.

**Clause 146**

**ASSESSMENT NOTICES**

*Amendment made:* 55, in clause 146, page 81, line 3, leave out “with the day on which” and insert “when”—(Margot James.)

This amendment is consequential on Amendment 71.

Clause 146, as amended, ordered to stand part of the Bill.

Clause 147 ordered to stand part of the Bill.

**Clause 148**

**ENFORCEMENT NOTICES**

*Question proposed,* That the clause stand part of the Bill.

**Louise Haigh:** Earlier, we debated the requirement for law enforcement agencies to conduct data protection impact assessments ahead of developing or using any new filing system, and we debated several examples of what those filing systems or methods of data collection could be, including automated facial recognition software, automatic number plate recognition and the use of algorithms to determine decisions made in the criminal justice system.

In relation to the clause, the Information Commissioner has requested that she be given the power to impose corrective measures where necessary, when a data protection impact assessment has revealed that the processing of that personal data is of high risk to individuals and where there are no measures to mitigate that risk in relation to law enforcement processing, as she has for other processing. She maintains that a different approach to law enforcement is not justified and might lead to adverse consequences in an important area affecting individuals. That is important because it gives weight to the important aspects raised earlier that require law enforcement agencies to conduct that DPIA. There is little point asking organisations and data controllers to conduct impact assessments and then, even when they are falling short dramatically, to let them carry on conducting assessments and collecting data in that way.

In evidence, the Information Commissioner has said that part 3 of the Bill “requires these types of assessment to be undertaken” and provides

“for requirements to consult the Commissioner where such a high risk is present but measures cannot be put in place to mitigate these. They also provide requirements for the Commissioner to use her corrective powers in relation to GDPR but the way the Bill is drafted these corrective powers will not be available in relation to concerns arising from a DPIA involving law enforcement processing. Nor are there any powers available to ensure that the Information Commissioner can take action if a DPIA for law enforcement processing is not carried out when required.”

Not only are there no enforcement powers if the DPIA is conducted and falls short, but the Information Commissioner is not provided with any powers under this legislation to compel a DPIA to take place. Given, as we discussed earlier, the serious threats not just to data rights, but to prevention with respect to an individual’s rights to liberty and freedom, it is very serious indeed if
law enforcement agencies will be able to carry out impact assessments without any adherence to the provisions in the Bill.

The Information Commissioner says:

“Having the ability to issue corrective measures based upon the DPIA or indeed requiring a DPIA to be undertaken when it should have been, is an important measure which is missing in relation to law enforcement processing”.

The commissioner has raised her concerns with the Government and suggested drafting solutions. Will the Minister clarify why those were not introduced in Committee?

**Margot James:** The clause gives the commissioner the power to issue an enforcement notice, which requires a person to take steps or refrain from taking steps specified in the notice. For example, the commissioner can use an enforcement notice to compel a data controller to give effect to a data subject if they have otherwise failed to do so. Section 40 of the Data Protection Act 1998 made similar provision. In respect of the hon. Lady’s questions concerning the law enforcement aspects of the clause and the need for impact assessments, and the powers that the ICO might need to ensure that those impact assessments are done and are appropriate, I will have to write to her on the details of those latter points.

**Question put and agreed to.**

Clause 148 accordingly ordered to stand part of the Bill.

**Clause 149**

**Enforcement notices: supplementary**

Amendment made: 56, in clause 149, page 83, line 36, leave out “with the day on which” and insert “when”.—(Margot James.)

This amendment is consequential on Amendment 71.

Clause 149, as amended, ordered to stand part of the Bill.

**Clause 150**

**Enforcement notices: rectification and erasure of personal data etc**

**Question proposed,** That the clause stand part of the Bill.

**Liam Byrne:** The clause bites on the question of individuals’ rights to the erasure of personal data and rectification. I want to give the Minister an opportunity to update the Committee on her conversations with media, culture and other organisations about how she is going to balance the implementation of clause 150 with the ambitions of those organisations to protect archives—not just archives of very large sets of artefacts, such as the Natural History Museum, but those that are run by News UK or Trinity Mirror or the BBC.

The risk that is obviously posed by those organisations is that they often rely on very good, detailed and often quite old archives of news information. The scenario that was put to us last night by lawyers representing a number of those organisations that wanted to give us their views about clauses 168 and 169 was that successful journalism—whether The Daily Telegraph or the Swindon Advertiser—will often rely on excellent archives.

If rich individuals are seeking to create a different truth and a different history, and to exercise their rights under the clause, a risk will be created for those media organisations. I am more worried about the media organisations’ rights than I am about the Natural History Museum and the BBC, because I think the Minister’s Department will do a good job of working out where to put that grey line round what should be protected and what is up for grabs. The example put to us last night was of rich individuals seeking to create a different kind of history—a different kind of past—to bend deliberately the future of reporting by eradicating a record that might be true. The risk that was put to us is that, very often, newspaper legal directors—the poor things often have to advise on this decision—will sometimes conclude that the game is just not worth it and therefore give in to the rich individual to avoid damaging and expensive legal action and delete the records from their archives.

This is a difficult area, where balances have to be struck, but it is a form of litigation that will doubtless continue into the future. We might have just decided to deny access to ordinary people to correct media malpractice, but rich individuals will continue to bring their cases. Will the Minister tell us how the balance will play out in practice? How do we protect the rights of news organisations to run good archives for the benefit of public interest journalism in the future?

**Margot James:** The clause makes additional provision for enforcement notices where the subject matter of the notice relates to the controller or processor’s failure to comply with the data protection principle of ensuring accuracy. The clause may also apply where a controller or processor has failed to comply with the data subject’s rights on rectification, erasure or restriction of processing under articles 16 to 18 of the general data protection regulation.

We touched on the issue of archives in one of the Committee sittings last week. I explained to the Committee that there is protection for archives under the GDPR, whether they be those of news organisations or of academic sources. We are aware of the concerns expressed by organisations representing archives, and I agree with the right hon. Gentleman that quality journalism often depends on the use of such archives. However, I assure him that my Department will defend the rights of journalists and the press as tenaciously as we would defend the rights of archivists in the great museums of our country against the distortions that he gave as examples of people perhaps wanting to use the right to be forgotten in an excessive manner and in a bid to rewrite history. We are aware of such individuals, and we are comfortable that the GDPR prevents those abuses.

**Question put and agreed to.**

Clause 150 accordingly ordered to stand part of the Bill.

Clauses 151 and 152 ordered to stand part of the Bill.

**Clause 153**

**Powers of entry and inspection**

**Question proposed,** That the clause stand part of the Bill.

**Liam Byrne:** Again, on this point, we would benefit from some clarification from the Minister. The story that broke this morning was that the Information
Commissioner had, in effect, to go to court to get her warrant to investigate what Cambridge Analytica was up to. There was some speculation as to why Facebook was unable to exercise some contractual rights and turn up at the offices of Cambridge Analytica to conduct an inspection. The reports are that, as the situation played out, the Information Commissioner had to tell Facebook legal officers to stand down and to stop what they were doing. As it happened, Facebook wisely decided to follow the Information Commissioner’s orders.

A matter of great concern is that the Information Commissioner has to go through what sounds like a laborious process to get the warrant needed to conduct an investigation that is obviously in the public interest. When we secure, for example, emergency injunctions to stop the publication of material that people do not want published, or when magistrates issue search warrants, most of us with experience of this at a local level would observe that such warrants are often issued in a much faster and less high-profile way than the process the Information Commissioner appears to have to go through.

In effect, Cambridge Analytica has had 48 hours’ notice of the Information Commissioner’s concerns—[Interruption.] I am sorry, but I do not know whether the Minister wants to intervene on that—

The Chair: Order. There is confusion on the Front Bench. Please continue, Mr Byrne.

Liam Byrne: I am sorry, Mr Hanson. I was not sure whether the Home Office Minister wanted to clarify that point. We know that warrants have to be sought and judicial oversight is important, but the process appears slightly cumbersome. I wonder whether the Minister can tell us whether she is satisfied that the process and the powers that we will equip the Information Commissioner with are as smooth and slick as the new enforcement environment requires.

3.45 pm

Margot James: I remind the right hon. Gentleman. I was not sure whether the Home Office Minister wanted to clarify that point. We know that warrants have to be sought and judicial oversight is important, but the process appears slightly cumbersome. I wonder whether the Minister can tell us whether she is satisfied that the process and the powers that we will equip the Information Commissioner with are as smooth and slick as the new enforcement environment requires.

The Chair: With this it will be convenient to discuss Government amendments 57 and 180.

Margot James: As part of the Information Commissioner’s suite of corrective powers, she can issue penalty notices to data controllers requiring them to pay a fine. Fines can be issued where a controller has failed to comply with a previous notice or where significant breaches of data protection legislation have taken place. Members will be aware from our debate this afternoon that the maximum such penalty will increase from £0.5 million to £17 million, or 4% of global turnover, for the most serious breaches.

When imposing a penalty for breaches of the GDPR, the commissioner must follow the procedures set out in article 83 of the GDPR, which include acting on a case-by-case basis; ensuring that the fine is effective, proportionate and dissuasive; and taking into account various factors. Because law enforcement and intelligence services processing falls outside the scope of the GDPR, the clause makes parallel provision in respect of breaches of those parts of the Bill, including by listing matters that the commissioner must take into account when deciding whether to issue a fine for that type of processing and when determining the magnitude of that fine.

Government amendments 179 and 180 make it clear that, when considering a person’s failure to comply with notices—an information notice, for example—the commissioner is to have regard to the matters listed in article 83(2) of the GDPR and, in relation to law enforcement processing and intelligence processing, to clause 154(3) and (4) of the Bill. Clause 154 prescribes such requirements only for decisions regarding the issuing of a monetary penalty notice in relation to certain failings. The commissioner has powers to prepare guidance on how she uses her enforcement powers, so she could decide, as a matter of policy, to have regard to those matters in relation to other failings. However, the Government’s view is that there should be a requirement for her to do so in the Bill.

Government amendment 57 makes an addition to clause 154(3)(c) to ensure that the Information Commissioner takes into account any actions the controller has taken to mitigate not only damages, but distress suffered by the data subject. The amendment will bring the clause into line with other similar clauses in the Bill, where the Information Commissioner must take into account damage or distress caused. They include clause 149 regarding enforcement notices, where the Information Commissioner must take into account the magnitude of the damage or distress caused by the controller.

I am
[Margot James]

sure right hon. and hon. Members will agree that providing consistency across the Bill is important; the amendment is a step to ensure that that is provided.

Amendment 179 agreed to.

Amendments made: 57, in clause 154, page 86, line 10, at end insert “or distress”.

This amendment, in or for consistency with Clause 149(2). It requires the Commissioner, when deciding whether to give a penalty notice to a person in respect of a failure to which the GDPR does not apply and when determining the amount of the penalty, to have regard to any action taken by the controller or processor to mitigate the distress suffered by data subjects as a result of the failure.

Amendment 180, in clause 154, page 86, line 28, at end insert—

“(3A) Subsections (2) and (3) do not apply in the case of a decision or determination relating to a failure described in section 148(5).” —(Margot James.)

See the explanatory statement for amendment 179.

Question proposed, That the clause, as amended, stand part of the Bill.

Louise Haigh: I am sorry to labour the point; it is pertinent to the clause but also relates to the debate that we just had on information notices. The Minister has failed to set out why the Government have removed the custodial sentence as an enforcement power of the Information Commissioner when data controllers or processors breach information notices. The Minister said earlier that she does not accept that it is the Information Commissioner’s view that that weakens the existing data protection regime, but the commissioner explicitly set that out in her written evidence to the Committee:

“The new approach in the Bill of failure to comply with an IN no longer being a criminal offence but punishable by a monetary penalty issued by the ICO is likely to be less of a deterrent”.

We very much welcome the increased penalty as a sanction by the Information Commissioner, but the Minister has so far failed to set out why she has removed that custodial sentence, which, as the Information Commissioner has laid out, is a serious deterrent. That could weaken her abilities to investigate complex situations and, as I mentioned earlier, it is in direct contrast to the Irish Government’s approach, which carries a fine but also a custodial sentence of up to five years’ imprisonment if the data controller fails to comply with an information notice.

In written evidence, again, the Information Commission suggests that the Government’s approach pales in comparison to that taken by Ireland. Will the Minister take this opportunity to explain why she has so significantly weakened the Information Commissioner’s important powers?

Margot James: The clause replicates section 55(a) of the 1998 Act, which gives the commissioner a power to serve a monetary penalty, requiring the data controller to pay the commissioner an amount determined by the commissioner. The maximum penalty is specified in clause 156. Before the commissioner can issue a penalty notice, she must be satisfied that a person has failed to comply with certain provisions of the GDPR or the Bill, or has failed to comply with an information notice, assessment notice or enforcement notice.

Clearly, it is up to the commissioner to decide whether a penalty notice is appropriate. She has stated: “I am about putting the...citizen first. We can’t lose sight of...It’s true we’ll have the power to impose fines much bigger than the £500,000 limit the DPA allows us.”

Daniel Zeichner: For reasons that are entirely understandable, my constituents in Cambridge take a particularly close interest in some of the things that have been happening with Cambridge Analytica this week. They will be astonished that the Minister does not seem to be answering the question raised by my hon. Friend the Member for Sheffield, Heeley. Financial penalties, yes, but criminal proceedings surely should be uppermost when we have seen these dreadful things that have been going on.

Margot James: I was coming on to answer the hon. Member for Sheffield, Heeley, but as the hon. Member for Cambridge has raised her question again, I will jump to it. We are not removing all criminal powers under this new legislation. Under paragraph 2 of schedule 15, the commissioner may enforce assessment notices. That power includes the new offence of obstructing a warrant, which is a criminal offence, so criminal offences do remain. As I said, we are looking at the commissioner’s desire for stronger powers in certain areas, but under the current law there is a criminal sanction only for non-compliance with a notice, and that offence is not used. A civil penalty is a better way forward and is provided as the appropriate sanction by the GDPR itself.

Louise Haigh: The Minister has just confirmed that under the existing arrangements a custodial sentence is the maximum penalty if an individual fails to comply with an information notice. She has not given a coherent reason why she is removing that through the Bill. Is she really arguing that criminal sanctions are less of a deterrent than civil? That is a direct contradiction of the Information Commissioner’s evidence.

Margot James: I have just been advised that the existing law is non-custodial criminal sanctions. I have referred to the criminal sanctions with respect to assessment notices, and I will get back to the hon. Lady on the question of the sanctions on the information notices that she has asked about. I am told what I am told; the existing law is non-custodial.

Question put and agreed to.

 Clause 154, as amended, accordingly ordered to stand part of the Bill.

Schedule 16

PENALTIES

Amendments made: 123, page 203, line 26, leave out “with the day after” and insert “when”.

This amendment is consequential on Amendment 71.

124, page 204, line 10, leave out “with the day on which” and insert “when”.

This amendment is consequential on Amendment 71.

125, page 205, line 5, leave out “with the day after the day on which” and insert “when”.

This amendment is consequential on Amendment 71.

126, page 205, line 37, leave out “controller or processor” and insert “person to whom the penalty notice was given”.—(Margot James.)

This amendment is consequential on Amendment 52.

225 226
Clause 156

MAXIMUM AMOUNT OF PENALTY

Question proposed, That the clause stand part of the Bill.

Liam Byrne: I think we could all do with a bit of clarity, which did not quite emerge in the last debate. My hon. Friend the Member for Sheffield, Heeley, makes an important point: in light of this week’s news, there is real concern that the maximum possible sentences should be on the books to punish people who try to get in the way of investigations by the Information Commissioner. Can the Minister say whether the Information Commissioner is currently able to prosecute people for getting in her way, and whether they could go to jail? That would be clarification No. 1. Clarification No. 2 would be whether, under the Bill the Minister is asking us to agree, that custodial sentence would still remain.

Margot James: I understand that under the current law there are no custodial sentencing provisions, so therefore I cannot argue that they will remain. That does not seem logical at all. The existing DPA offences are for fines only, according to section 60 of the Data Protection Act 1998.

Question put and agreed to.

Clause 156 accordingly ordered to stand part of the Bill.

Clause 157

FIXED PENALTIES FOR NON-COMPLIANCE WITH CHARGES REGULATIONS

Question proposed, That the clause stand part of the Bill.

Liam Byrne: Given the clarity that the Minister has now furnished for the Committee, and given the scale of wrongdoing that is alleged about Cambridge Analytica and potentially Facebook this week, the question on clause 157 is whether she is satisfied that financial penalties are going to do the job in the years to come. Otherwise, is this a clause on which we need to reflect on Report if not now so that if custodial sentences are not currently available, we might consider introducing them for people who appear determined to move heaven and earth to get in the way and obstruct an Information Commissioner inquiry? Could we perhaps come back to that on Report, rather than simply rely on sanctions such as fixed penalty notices?

4 pm

Margot James: I have mentioned before to the right hon. Gentleman that there are criminal offences set out in the Bill, such as an offence of obstructing a warrant, which would enable the ICO to go in and exercise search and seizure powers. Although obstruction carries potential fines and a criminal record, I do not believe that it carries the threat of a custodial sentence, which is no change from the current situation.

As I have said before, and as my right hon. Friend the Secretary of State said yesterday, we are reviewing the enforcement powers of the ICO, and we are working with the commissioner to ensure that we get the whole suite absolutely right. I cannot say any more than I already have on that point.

Question put and agreed to.

Clause 157 accordingly ordered to stand part of the Bill.

Clause 158 ordered to stand part of the Bill.

Clause 159

GUIDANCE ABOUT REGULATORY ACTION

Amendment made: 58, in clause 159, page 89, line 37, leave out “a” to end of line 38 and insert “person to make oral representations about the Commissioner’s intention to give the person a penalty notice;”—(Margot James.)

This amendment is consequential on Amendment 52.

Clause 159, as amended, ordered to stand part of the Bill.

Clauses 160 to 163 ordered to stand part of the Bill.

Clause 164

ORDERS TO PROGRESS COMPLAINTS

Amendment made: 59, in clause 164, page 93, line 4, leave out “with the day on which” and insert “when”

This amendment is consequential on Amendment 71.—(Margot James.)

Clause 164, as amended, ordered to stand part of the Bill.

Clauses 165 to 167 ordered to stand part of the Bill.

Clause 168

PUBLISHERS OF NEWS-RELATED MATERIAL: DAMAGES AND COSTS

Question put, That the clause stand part of the Bill.

The Committee divided: Ayes 7, Noes 10.

Division No. 12]

AYES

Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren

Murray, Ian
Snell, Gareth
Zeichner, Daniel

NOES

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

Jack, Mr Alister
James, Margot
Lopez, Julia
Warman, Matt
Wood, Mike

Question accordingly negatived.

Clause 169

PUBLISHERS OF NEWS-RELATED MATERIAL: INTERPRETIVE PROVISIONS

Question put, That the clause stand part of the Bill.

The Committee divided: Ayes 7, Noes 10.
The Government recognise that it is important to protect whistleblowers. There is a protection in clause 170 for whistleblowers bringing forward information that is “justified as being in the public interest.”

The argument put to us by Public Concern at Work and others is that that approach is unlikely to be effective. We are told that there will be a new test in law, which will therefore require guidance from the courts. Until that time, the precise meaning will obviously be a bit moot, and the scope of the situations that the Government seek to protect will remain a little uncertain. That uncertainty and ambiguity will jeopardise an individual who might have something important to bring to the attention of the outside world.

Exceptions to violations in personal data confidentiality were recently considered by the Government in section 58 of the Digital Economy Act 2017, which provided a far more comprehensive list of exceptions. Where there is overlap between the Bill and the Digital Economy Act, appears that the Act deals much more satisfactorily with whistleblowers.

I remind the Committee that section 58 of the Act says that the offence does not apply to a disclosure “which is a protected disclosure for any of the purposes of the Employment Rights Act 1996 or the Employment Rights (Northern Ireland) Order 1996 (SI 1996/1919 (NI 16)).”

We therefore have a pretty well established and grounded definition of exceptions. Indeed, it was so well defined and grounded that the Government decided to use that definition in the 2017 Act. It is not clear why the Bill seeks to create alternative definitions and therefore the need for alternative tests and guidance in the courts when we have a definition we can rely on.

The Opposition amendment would return us to what we think was sensible drafting in the Digital Economy Act. That Act is not ancient history—it was only 12 months ago. Otherwise, the risk is that the Government, employers, courts and trade unions will get into an awful muddle as they try to understand which legislation protects whistleblowers in new circumstances. None of us wants to create a situation of uncertainty and ambiguity that stops whistleblowers from coming forward with important information.

I therefore hope we can have a useful debate about why the Government have chosen to introduce new definitions when it is not clear that they are improvements on well-established employment law that dates back to the Employment Rights Act 1996. Let us hear what the Minister has to say, but I hope the Government reflect on the arguments we rehearse this afternoon and introduce further enhancements and perfections on Report.

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): The right hon. Gentleman is correct: it is essential that we do not create an offence in the clause that will snare whistleblowers. I am sure the Committee shares that goal. Indeed, if we created such an offence, whistleblowers would no longer be whistleblowers—a qualifying disclosure would no longer be a qualifying disclosure if it were an offence under different legislation, including the Bill.

We will listen carefully to what the Minister says, but, to come at it from a slightly different angle, as I understand it, the Employment Rights Act currently requires a
“reasonable belief” by the worker making the whistleblowing disclosure that it is in the public interest to disclose that information. That seems a slightly easier test than the one contained to a defence in subsection (2) of the clause, which requires not a “reasonable belief”—those words do not appear—but proof that disclosure was justified in the public interest. There is also a contrast with subsection (3), where a reasonable belief test is applied to a defence but only in circumstances of publication of either journalistic, artistic or literary material.

It is not clear to me why there is a reasonable belief test in subsection (3) but not in subsection (2). I am interested to hear what the Minister has to say about that distinction.

Margot James: The amendments concern offences relating to personal data provided for by part 6 of the Bill. Hon. Members will be aware that the offence of unlawful obtaining of personal data has been carried over and updated from the 1998 Act to include the unlawful retention of personal data without the controller’s consent. By contrast, the offence of re-identification of de-identified personal data is new to data protection legislation, underlining our intention to bring data protection laws up to date with the digital age.

Amendment 157 would add an additional defence to clause 170 where the conduct is in the process of a disclosure by an employee raising public interest concerns about wrongdoing or malpractice to the extent that such disclosures would be protected by the Employment Rights Act 1996 and equivalent legislation for Northern Ireland. Amendment 158 adds the same defence to clause 171.

I share the sentiment of the amendments, but believe they are unnecessary. Clauses 170 and 171 provide defences in cases where the processing is necessary for the prevention or detection of crime or can be justified as being in the public interest. We believe that the crime prevention defence would cover a disclosure by an employee who suspected that an offence had been committed, and that the flexible public interest defence would encapsulate the other non-criminal activities envisaged by the amendments. In particular, as set out in section 43B of the Employment Rights Act 1996 and article 67B of the Employment Rights (Northern Ireland) Order 1996, a disclosure is protected in the first place only if the disclosing worker reasonably believes the disclosure to be in the public interest.

4.15 pm

Stuart C. McDonald: This is a narrow question that I raised in my speech. There is a “reasonable belief” test in the 1996 Act. It is easier for someone to prove that they had a reasonable belief that a disclosure was in the public interest than to prove that it was in the public interest. That slight difference in wording may be significant. There are in fact two different tests in the clause, so I wonder whether the Minister might look at that again.

Margot James: I referred to the public interest defence as a flexible defence that would encapsulate non-criminal activities. I do not know whether that satisfies the hon. Gentleman, but a flexible public interest defence is indeed required.

For those reasons, I reassure hon. Members that a further defence providing for whistleblowing is unnecessary. It is telling that there is no such defence in section 55 of the 1998 Act, and we are not aware of any problems with its operation. Hon. Members mentioned section 58 of the Digital Economy Act 2017. That is a difficult comparison. Unlike clauses 170 and 171, section 58 does not contain a straightforward public interest defence, so, unlike the offences in the Bill, there may be no alternative protection for such disclosures. I hope I have given hon. Members sufficient reassurance that they feel confident withdrawing their amendments.

Liam Byrne: I am grateful to the Minister for that reply. She says that she wants to try to update the legislation. I understand what she is trying to do and why she does not accept that there is a complete parallel with the Digital Economy Act. None the less, the new definition will need to be tested in court, new guidance will need to be issued and new ambiguity will therefore be created, which brings with it the risk that important whistleblowers will be dissuaded from bringing forward information that is in our interest and letting it see the light of day.

I hope the Minister reflects on that further. She seeks to create an extension in law to ensure that there is a public interest definition in the round—I can see the enlargement that she is trying to make—but I hope she reflects before Report stage on the challenge that new definitions will have to be tested in court, which will create ambiguity and risk. I do not think she wants to create that risk, but the strategy she sets out does not completely delete it and it remains a concern. I will happily withdraw the amendment, but I ask the Minister to reflect on that point before Report.

Margot James: I am happy to reflect on what the right hon. Gentleman proposes. The last thing we want is to have any chilling effect on would-be whistleblowers.

Liam Byrne: I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 170 ordered to stand part of the Bill.

Clause 171

Re-identification of de-identified personal data

Question proposed, That the clause stand part of the Bill.

Darren Jones (Bristol North West) (Lab): It is a pleasure to serve under your chairmanship this afternoon, Mr Streeter. I want to pursue the debate on the re-identification of de-identified personal data because, as the Minister pointed out, under the general data protection regulation, the idea of pseudonymised data comes into the law for the first time. For example, if my name, as my personal data, is turned into #365, it has been pseudonymised, and the question is whether #365 can be unlocked to identify the name “Darren Jones”. Pseudonymising is distinct from anonymising, which cannot be unlocked.
The question has come up a lot in the Select Committee on Science and Technology, in various contexts. I had a conversation with the Minister and her officials in the Select Committee about one scenario—the use of genetic data in the health service, where lots of data from individuals is pooled together for the purpose of learning about trends. It may be re-applied to the individual in the delivery of care. Another example might involve Facebook clients being able to upload customer lists on to the Facebook advertising profile. Each name would be hashed—pseudonymised—but ultimately targeted advertising could be pushed through to the individual’s profile.

Both those scenarios raise a policy question about the end of the process, when it comes back to the individual—the information has been personally identifiable, then is pseudonymised in a pooled way, and is then re-identified. Will those issues give rise to an offence under the part of the Bill that we are considering, and should consent be different, with the potential for pseudonymised data to be re-identified made clear to the end user? The reason I have not tabled any amendments to deal with this point is that I do not know the answer, but I should welcome the Minister’s views, and perhaps a commitment to have a conversation either with the Information Commissioner or the new data and artificial intelligence ethics unit about different types of consent where data is pseudonymised and then re-identified, either for health purposes or targeted advertising.

The Chair: I hope the Minister understood all that.

Margot James: I am sure you did, Mr Streeter.

Clause 171 creates a new offence of knowingly or recklessly re-identifying information that has been de-identified without the consent of the controller who de-identified the data. It is a response to concerns about the security of de-identified data held in online files. For example, recommendations in the review of data security, consent and opt-outs by the National Data Guardian for Health and Care call for the Government to introduce stronger sanctions to protect de-identified patient data, to which I think the hon. Member for Bristol North West was referring.

Subsection (3) provides the defendant with a defence if he or she can prove that re-identification was necessary for the purposes of preventing crime or complying with a legal obligation, or that it was justified in the public interest. Subsection (4) provides further defences where the defendant can prove they reasonably believed that they had or would have had the consent of the data subjects to whom the information relates or of the data controller responsible for de-identifying the information, or that they acted for the special purposes, with a view to publication, and the re-identification was reasonably believed to be justified in the public interest, or if the effectiveness testing conditions in clause 172 were met.

I have perhaps strayed rather far into the matter of defences in answering the hon. Gentleman, and may not have entirely satisfied him as to his question. If he is agreeable I will write to him, and get from my officials the latest as to the oversight of the important questions he raises.

Louise Haigh: My hon. Friend the Member for Bristol North West has raised important questions about social media providers. Before I entered this place, I worked in the insurance industry. Will the Minister confirm whether insurers would be covered by the clause if they re-identified individuals from datasets to inform the pricing of risk? That is potentially serious when considering the implications of loyalty card, bank or shopping information for health insurance.

Margot James: I will have to write to the hon. Lady on that. I do not think it would provide cover for insurance companies in those circumstances, but I would like to double-check before I give a definitive answer to her question.

Question put and agreed to.

Clauses 171 accordingly ordered to stand part of the Bill.

Clauses 172 to 176 ordered to stand part of the Bill.

Clause 177

JURISDICTION

Darren Jones (Bristol North West) (Lab): I beg to move amendment 151, in clause 177, page 102, line 13, at end insert—

“(4) Notwithstanding any provision in section 6 of the European Union (Withdrawal) Act 2018, a court or tribunal shall have regard to decisions made by the European Court after exit day so far as they relate to any provision under this Act.”

For fear of sounding like a broken record, my arguments in favour of the amendment are broadly similar to those for amendment 152—in seeking to assist the Government in our shared aim of getting a decision of adequacy with the European Commission, it would be helpful to set out in the Bill our commitment to tracking and implementing European jurisprudence in the area of data protection. Members will remember that amendment 152 dealt with the European data protection board. Amendment 151 makes the same argument, but in respect of the European Court.

I appreciate that there may be some political challenges in stating the aim that the UK will mirror the European Court’s jurisdiction, but the reality is that developing European data protection law, either directly from the courts or through the European data protection board, will in essence come from the application of European law at the European Court of Justice. The amendment does not seek to cause political problems for the Government, but merely says that we ought to have regard to European case law in UK courts, in order to provide the obligation to our learned friends in the judiciary to have regard to European legal decision making and debates in applying European-derived law in the United Kingdom. This short amendment seeks merely to put that into the Bill, to assist the Government in their negotiations on adequacy with the European Commission.

Liam Byrne: I would like to say a word in support of this important amendment. We had a rich and unsatisfactory debate on the incorporation of article 8 of the European charter of fundamental rights into British law. We think that that would have helped the Government considerably in ensuring that there is no divergence between the European data protection regime
and our own. If the Government are successful, they will operate on different constitutional bases, and there is therefore a real risk of divergence over the years to come. I think that everyone on the Committee is now pretty well versed in the damage that that would do to British exports, many of which are digitally enabled. This is a really helpful amendment. It tries to tighten to lockstep that we have to maintain with European data protection regimes, which will be good for exports, services and the British economy, and the Government should accept it.

Margot James: When we leave the European Union, the direct jurisdiction of the Court of Justice of the European Union in the UK will come to an end. Clause 6 of the European Union (Withdrawal) Bill gives effect to that and takes a clear and logical approach to how our domestic courts should approach the case law of the CJEU as a result. In short, where a judgment precedes our exit, it is binding on courts below the Supreme Court. Where a judgment post-dates our exit, our courts may have regard to it if they consider it appropriate, but EU law and the decisions of the ECJ will continue to affect us. The ECJ determines whether agreements that the EU has struck are legal under the EU’s own law. If, as part of our future partnership, Parliament passes an identical law to an EU law, it may make sense for our courts to look at the appropriate ECJ judgments so that we interpret those laws consistently, but our Parliament would ultimately remain sovereign.

The approach is sensible and realistic. Opposition Members have suggested that if the UK is to achieve future negotiations with the EU, we must follow the jurisprudence of the ECJ. We do not believe this to be the case. There are a number of existing precedents where the EU has reached agreements with third countries that provide for a close co-operative relationship without the CJEU having direct jurisdiction over those countries. It is worth quoting directly from the European Union (Withdrawal) Bill, which states: “A court or tribunal need not have regard to anything done on or after exit day by the European Court, another EU entity or the EU but may do so if it considers it appropriate to do so.”

I should make it clear that the provision does not seek to legislate for the content of a withdrawal agreement or implementation period. If there is a role for the CJEU as part of the agreement, as has been set out in the joint report in relation to citizens' rights, it would be legislated for under the separate withdrawal agreement and implementation period, but it would not be right to try to legislate now in anticipation of a final legal text agreed with the EU on the terms of our withdrawal from the EU.

The position in the European Union (Withdrawal) Bill reflects the reality that in leaving the EU we will be ending the direct jurisdiction of the CJEU over our domestic courts while also allowing judges to take account of post-exit CJEU judgments. This is similar to how the UK courts can currently take into account judgments made by courts from other jurisdictions, although of course we recognise that as the text of our law and EU law will at the outset be the same or substantially similar in many cases, it is highly likely in practice that our courts may find it helpful to look at the CJEU judgments, and that is perfectly legitimate and sensible for them to do so.

Ian Murray (Edinburgh South) (Lab): The Prime Minister said in her Mansion House speech earlier this month that as a country we may have to stay under the jurisdiction of the CJEU for the purposes of organisations such as Euratom and other EU-wide organisations that the UK may wish to remain part of. Is the Minister saying that this is a possibility with regard to data protection laws in this legislation?

Margot James: The future of our membership of the European Data Protection Board will be subject to negotiations. I cannot prejudge how those negotiations will develop and finalise in respect of our membership of that important body.

Ian Murray: Am I right in saying that the Minister is not ruling it out as part of the legislation?

Margot James: I would not rule it out, but the negotiations are between two parties, so however much we may wish to maintain our membership of the European Data Protection Board, that might not be something that the EU will grant us. As I say, it is a matter for negotiation and I am sure things will become clearer over the next 12 months. To take an approach now that would require our courts to follow future case law of the CJEU, even if only in some areas, would place limitations on the discretion and independence of our courts.

Liam Byrne: The Minister is trying to protect a discretion that sounds like the defence of a right to depart from EU case law to such an extent that we might jeopardise an adequacy agreement. Surely the point of this amendment is to keep us in lockstep, to de-risk that adequacy agreement for the years to come. That surely must be an object of her Government’s policy.

Margot James: The Government are absolutely committed to getting an adequacy agreement. The Prime Minister has said she wishes to go beyond adequacy in the negotiations. I would like to reassure the right hon. Gentleman that the very opposite is the case. Our courts can have regard to, and that is good enough. There is no reason for this to be different in the area of data protection from what it might be in any other area.

The provision has been discussed at length and agreed to by the House. Hon. Members will be aware that the other place is now scrutinising the EU (Withdrawal) Bill and has focused on this very matter. There is broad agreement that we need to consider how best to ensure that the Bill achieves the policy aim with sufficient clarity. We want to reach agreement on a proposition that commands the greatest possible support. We should, however, be wary of seeking to provide for something that alters the underlying policy in a way that binds or
steers our courts towards a particular outcome, for example, by saying that they must have regard in only certain areas of law.

**Liam Byrne:** I do not quite follow the Minister’s argument. On the one hand, she says that it is the object of Government policy to secure an adequacy agreement and presumably keep that adequacy agreement, if not, indeed, go beyond it. She is now seeking to defend a flexibility that would allow some kind of departure from European norms. I cannot understand how she can quite want her cake and eat it.

**Margot James:** Courts will be allowed to follow the jurisprudence of the ECJ in this area of data protection. Nothing I am saying is prompting a departure from that position. We see the amendment as going further than we would like to go. By contrast, the Government’s proposed approach to CJEU oversight respects the referendum result and is clear, consistent and achievable.

**Darren Jones:** The Minister gave a full answer, largely in agreement with the points I made.

**Margot James:** Not much; not with those.

**Darren Jones:** I agree. I would therefore invite the Government to reconsider their position and support the amendment, because it reflects what is in the EU (Withdrawal) Bill, it talks about having regard to ECJ jurisprudence in future and, as the Minister pointed out, Government policy and the Government’s intention are that we are going to end up in that position anyway. By putting that in the Bill, we would put it into law and give a very clear signal to our colleagues in the European Union that that is our intention and we will stand by it.

The Minister’s arguments do not seem to stack up. If I were saying in the amendment that we must apply ECJ case law directly and that the UK courts had no power to disregard EU jurisprudence I would probably agree, but that is not what it seeks to do. I am not convinced it goes beyond the Government’s policy position nor what is said in the EU (Withdrawal) Bill. I merely seek to help the Government by making this simple amendment to the Bill. With your permission, Mr Streeter, I will push it to a vote.

**Question put,** That the amendment be made.

The Committee divided: Ayes 9, Noes 10.

**Division No. 14**

That the amendment be made.

**AYES**

Byrne, rh Liam
Elmore, Chris
Haigh, Louise
Jones, Darren
McDonald, Stuart C.

**NOES**

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel
Jack, Mr Alister
James, Margot
Lopez, Julia
Warman, Matt
Wood, Mike

**Question accordingly negatived.**

Clause 177 ordered to stand part of the Bill.
Clause 178 ordered to stand part of the Bill.

**Clause 179**

**REGULATIONS AND CONSULTATION**

**Amendment made:** 62, in clause 179, page 103, line 35, at end insert—

“( ) If a draft of a statutory instrument containing regulations under section 7 would, apart from this subsection, be treated for the purposes of the standing orders of either House of Parliament as a hybrid instrument, it is to proceed in that House as if it were not such an instrument.”—(Margot James.)

This amendment disapplies the procedure for hybrid instruments in the House of Lords (and any similar procedure that may be introduced in the House of Commons) in relation to regulations under Clause 7 (meaning of “public authority” and “public body” for the purposes of the GDPR).

Clause 179, as amended, ordered to stand part of the Bill.

Clauses 180 to 181 ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned.

—(Nigel Adams.)

4.41 pm

Adjourned till Thursday 22 March at half-past Eleven o’clock.
Written evidence reported to the House

DPB 38 Robin Makin (Chapter 4 part 4)
DPB 39 Lewis Silkin LLP
DPB 40 Society of Editors
DPB 41 Institute of Health Records and Information Management (IHRIM)
DPB 42 ISACA

DPB 43 National Pharmacy Association
DPB 44 Bates Wells Braithwaite
DPB 45 Media Lawyers Association
DPB 46 Information Commissioner’s Office supplementary written evidence
DPB 47 Global Witness
DPB 48 Evening Standard and Independent
DPB 49 Association for UK Interactive Entertainment
Public Bill Committee

DATA PROTECTION BILL [LORDS]

Seventh Sitting

Thursday 22 March 2018

(Morning)

CONTENTS

Schedule 17 agreed to, with amendments.
Clauses 182 to 204 agreed to, some with amendments.
Schedule 18 agreed to, with amendments.
Clauses 205 to 208 agreed to, some with amendments.
New clauses considered.
Adjourned till this day at Two o’clock.

PBC (Bill 153) 2017 - 2019
No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Monday 26 March 2018
The Committee consisted of the following Members:

*Chairs: David Hanson, †Mr Gary Streeter*

† Adams, Nigel (*Lord Commissioner of Her Majesty's Treasury*)
† Atkins, Victoria (*Parliamentary Under-Secretary of State for the Home Department*)
† Byrne, Liam (*Birmingham, Hodge Hill*) (Lab)
† Clark, Colin (*Gordon*) (Con)
† Elmore, Chris (*Ogmore*) (Lab)
† Haigh, Louise (*Sheffield, Heeley*) (Lab)
† Heaton-Jones, Peter (*North Devon*) (Con)
† Huddleston, Nigel (*Mid Worcestershire*) (Con)
† Jack, Mr Alister (*Dumfries and Galloway*) (Con)
† James, Margot (*Minister of State, Department for Digital, Culture, Media and Sport*)
† Jones, Darren (*Bristol North West*) (Lab)
† Lopez, Julia (*Hornchurch and Upminster*) (Con)
† McDonald, Stuart C. (*Cumbernauld, Kilsyth and Kirkintilloch East*) (SNP)
† Murray, Ian (*Edinburgh South*) (Lab)
† O’Hara, Brendan (*Argyll and Bute*) (SNP)
† Snell, Gareth (*Stoke-on-Trent Central*) (Lab/Co-op)
† Warman, Matt (*Boston and Skegness*) (Con)
† Wood, Mike (*Dudley South*) (Con)
† Zeichner, Daniel (*Cambridge*) (Lab)

Kenneth Fox, Committee Clerk

† attended the Committee
Amendments made: 128 in schedule 17, page 206, line 21, at end insert—
“Relevant health records
1A ‘Relevant health record’ means a health record which has been or is to be obtained by a data subject in the exercise of a data subject access right.”.
See the explanatory statement for Amendment 127.
Amendment 181 in schedule 17, page 207, line 22, leave out sub-paragraph (iii) and insert—
In a list of functions of the Secretary of State in relation to people sentenced to detention, this amendment removes a reference to section 73 of the Children and Young Persons Act 1968 (which has been repealed), and inserts a reference to Article 45 of the Criminal Justice (Children) (Northern Ireland) Order 1998 (which replaced it).
Schedule 17, as amended, agreed to.
Clause 182 ordered to stand part of the Bill.

Clause 183

REPRESENTATION OF DATA SUBJECTS

Amendments made: 63, in clause 183, page 105, line 42, leave out “80” and insert “80(1)”.
This amendment changes a reference to Article 80 of the GDPR into a reference to Article 80(1) and is consequential on NC2.
Amendment 64, in clause 183, page 105, line 44, leave out “certain rights” and insert “the data subject’s rights under Articles 77, 78 and 79 of the GDPR (rights to lodge complaints and to an effective judicial remedy)”.
In words summarising Article 80(1) of the GDPR, this amendment adds information about the rights of data subjects that may be exercised by representative bodies under that provision.
Amendment 65, in clause 183, page 106, line 7, leave out “under the following provisions” and insert “of a data subject”.
This amendment and Amendments 66, 67 and 68 tidy up Clause 183(2).
Amendment 66, in clause 183, page 106, line 9, at beginning insert “rights under”.
See the explanatory statement for Amendment 65.
Amendment 67, in clause 183, page 106, line 10, at beginning insert “rights under”.
See the explanatory statement for Amendment 65.
Amendment 68, in clause 183, page 106, line 11, at beginning insert “rights under”.—(Margot James.)
See the explanatory statement for Amendment 65.
Clause 183, as amended, ordered to stand part of the Bill.

Clause 184

DATA SUBJECT’S RIGHTS AND OTHER PROHIBITIONS AND RESTRICTIONS

Amendment made: 69, in clause 184, page 106, line 41, leave out “(including as applied by Chapter 3 of that Part)”.—(Margot James.)
This amendment is consequential on Amendment 4.
Clause 184, as amended, ordered to stand part of the Bill.
Ordered,
That clause 184 be transferred to the end of line 39 on page 105.—(Margot James.)
Clause 185

**FrameworK for Data Processing by Government**

*Question proposed.* That the clause stand part of the Bill.

**Liam Byrne:** I seek a bit of reflection and clarification from the Minister on this point. Clause 185 touches on the way in which the data processing regime operates for Her Majesty's Government. Within Her Majesty's Government, there are three very significant Departments that employ tens of thousands of people and process millions of bits of data every year. The three big data-processing parts of Her Majesty's Government are the Department for Work and Pensions, Her Majesty's Revenue and Customs and the Ministry of Defence. Very often, the formal data controller is the person who sits at the top of the office. Sometimes it is someone who has a relationship with the accounting officer at the top of the Department. The challenge that that creates for people who seek to exercise their data rights under this Bill is that subject access requests or other requests go into the Department, and it takes for ever to get a response. That is not a reflection on the quality of the civil servants who run the Departments; it is simply that they are sitting on top of millions of records—potentially hundreds of millions of bits of data—and the records may be held or processed by thousands of people operating at the frontline of a particular business.

The way we get around that problem in the national health service, which is probably the biggest Government data processor in the country, is that the data processor is often nominated at the trust level. The data controller may be a clinical commissioning group or an NHS hospital trust. The big Departments—the MOD, the MOD and HMRC—do not operate that strategy. It would be useful to know whether the Government, in the codes of practice that they issue to Departments, will persist with the practice of nominating data controllers at the very top, so that there will be a single data controller in a very large Department with ultimate responsibility for enforcing the Bill right the way through some of the biggest and most complex organisations on earth.

The Minister will know, having long been in her role, that all kinds of problems arise, particularly in the DWP, when information is sought, for example, for tribunal cases. If someone is bringing a tribunal case or wants to contest something about their data, sometimes the fastest way to do that is to file a subject access request just to get in one place how HMRC or the DWP did the calculations. Like the rest of us, the Minister will have had surgery cases along those lines. The first thing to do is to try to create a single picture of how the Department came to the decisions it made, which have a material impact on our benefits, health and wellbeing.

If the only way to assemble that full picture is to file a subject access request right the way up the chain to a civil servant at the top of the organisation, that is a very slow and fraught process. I invite the Minister to say a bit more about how she will reflect on a very different strategy for appointing and managing data controllers in the NHS, compared with the strategy that currently pertains in those three big administrative parts of Her Majesty's Government.

**Margot James:** The right hon. Gentleman makes a very good point. It might help if I say a little about the framework that the Secretary of State has to issue, as directed by clause 185, about the processing of personal data in connection with the exercise of functions within Government. Before the framework is issued, it has to be subject to parliamentary scrutiny. Some of these practical issues can be explored at that point. The framework will provide guidance to Departments on all aspects of their data processing. The content is being developed and we will definitely take into account the right hon. Gentleman's concerns.

*Question put and agreed to.*

**Clause 185 accordingly ordered to stand part of the Bill.**

Clause 186

**Approval of the Framework**

*Question proposed.* That the clause stand part of the Bill.

**Liam Byrne:** I am grateful to the Minister for taking those points on board. I suppose it begs the question of when she thinks we might see this framework. The process set out in the clause is a wise and practical course of action. We all have constituency experience that could have a bearing on how this piece of guidance is drafted and presented. We have the luxury of serving our constituents week in, week out. That is not a privilege that the civil servants who are asked to draft these frameworks enjoy.

It is important that the Minister goes through a good process, which allows her not to present the House with a fait accompli or something for an up and down motion. That will not be in any of our interests. My concern is how we practically operationalise this in a way that allows us continually to strengthen and improve the service that we provide to our constituents. It is very hard for us to do that if we have a data management regime operationalised by Her Majesty's Government that gets in the way.

When does the Minister expect to issue this framework? How will she ensure that there is a period of soft consultation with, perhaps, the Speaker's Committee here in the House so that we are not presented with a final draft of a document that we have 40 days to consider, moan about and make representations about, all of which will then basically be ignored because the approval process requires an up-down vote at the end.

**Margot James:** I cannot be precise as to when, but it will be a priority to issue the framework for all the reasons that the right hon. Gentleman set out. We intend to engage fully with officials across Government, in particular the Departments that he has mentioned, and will consult other areas of expertise and the Information Commissioner herself. Indeed, clause 185(5) sets a requirement for consultation. Most importantly, the framework will then come to Parliament for proper scrutiny. At that point the right hon. Gentleman will have every chance to contribute further to the practicality of establishing this framework as speedily as possible.

*Question put and agreed to.*

**Clause 186 accordingly ordered to stand part of the Bill.**
Clause 187

Publication and review of the Framework

Question proposed, That the clause stand part of the Bill.

Liam Byrne: The only issue arising from this clause is the frequency with which the Minister expects the framework to be updated. I welcome the steer that she has given the Committee about how clause 186(5) will be operationalised, but that does not quite get round the problem that I am concerned about. Sometimes, and it has been known to happen, regulations get somewhat hard wired before they are presented to the House. Although it is in the Bill, sometimes that 40-day consultation period does not provide an opportunity to review and update a measure if we do not think that it is practical.

If, for example, a code of practice is brought forward that says, “For the DWP, the data controller is going to be the accounting officer of the Department or someone associated with the accounting officer of the Department,” that is not going to be a practical strategy for operationalising this Bill within a Department as big and complicated as the DWP. So it may not be possible. We have to accept that. We have to accept the way statutory instruments are put through this place, and the political reality of that. Let us be mature about that. However, we have a belt-and-braces approach set out in clause 187, in that we have the chance to review it. Perhaps the Minister could say a word about how frequently she expects to review and update the legislation, so that it continually improves in the light of experience?

11.45 am

Margot James: Clause 187 requires the Secretary of State to publish the framework, and under clause 185 he must keep it under review, and commit to updating it as appropriate. Furthermore, although the Information Commissioner has to take the framework into account, were she investigating a data breach by a Government Department, for example, she might consider it relevant to consider whether that Department had applied the principles set out in the framework. She is also free to disregard the framework if she considers it irrelevant or getting in the way.

It will be a moving thing, and the legislation provides for the Secretary of State to keep it under continual review. If the right hon. Gentleman wishes to have some input before it arrives in the House in the form of a Statutory Instrument, I would be very happy to engage with him.

Question put and agreed to.

Clause 187 accordingly ordered to stand part of the Bill.

Clause 188 ordered to stand part of the Bill.

Clause 189

Publication and review of the Framework

Question proposed, That the clause stand part of the Bill.

Liam Byrne: We now come to offences, and crucially in clause 189, the question of penalties for offences. The real world has provided us with some tests for the legislation over the past few days. We have reviewed clauses 189 to 192 again in the light of this week’s news. Some quite serious questions have been provoked by the Cambridge Analytica scandal, and the revelations about the misuse of data that was collected through an app that sat on the Facebook platform.

For those who missed it, the story is fairly simple. A Cambridge-based academic created an app that allowed the collection not only of personal data but of data associated with one’s friends on Facebook. The data was then transferred to Cambridge Analytica, and that dataset became the soft code platform on which forensic targeting was deployed during the American presidential elections. We do not yet know, because the Mueller inquiry has not been completed, who was paying for the dark social ads targeted at individuals, as allowed by Cambridge Analytica’s methodology.

The reality is that under Facebook’s privacy policy, and under the law as it stood at the time, it is unlikely that the collection and repurposing of that data was illegal. I understand that the data was collected through an app that was about personality tests, and then re-deployed for election targeting. My understanding of the law is that that was not technically illegal, but I will come on to where I think the crime actually lies.

Julia Lopez (Hornchurch and Upminster) (Con): The right hon. Gentleman’s point makes it clear that the legislation is extremely timely. Does he not agree that that is why we are all here today—to try to improve the current situation?

Liam Byrne: Absolutely. That is why the European Commission has been working on it for so long. Today’s legislation incorporates a bit of European legislation into British law.

The crime that may have been committed is the international transfer of data. It is highly likely that data collected here in the UK was transferred to the United States and deployed—weaponised, in a way—in a political campaign in the United States. It is not clear that that is legal.

The scandal has knocked about $40 billion off the value of Facebook. I noted with interest that Mr Zuckerberg dumped a whole load of Facebook stock the weekend before the revelations on Monday and Tuesday, and no doubt his shareholders will want to hold him to account for that decision. I read his statement when it finally materialised on Facebook last night, and it concerned me that there was not one word of apology for what had happened or for Facebook basically facilitating and enabling it. That tells me that we simply will not be able to rely on Facebook self-policing adherence to data protection policies.

The hon. Member for Hornchurch and Upminster is absolutely right—that is why the Bill is absolutely necessary—but the question about the clause is whether the sanctions for misbehaviour are tough enough. Of the two or three things that concerned me most this week, one was how on earth it took the Information Commissioner so long to get the warrant she wanted to search the Cambridge Analytica offices. We think that the enforcement of the law is that that was not technically illegal, but I will come on to where I think the crime actually lies.
Commissioner the power to conduct such investigations. As we rehearsed in an earlier sitting, the proposed sanctions are financial, but the reality is that many of Cambridge Analytica’s clients are not short of cash—they are not short of loose change—so even the proposed new fines are not necessarily significant enough.

I say that because we know that the companies that contract with organisations such as Cambridge Analytica are often shell companies, so a fine that is cast as a percentage of turnover is not necessarily a sufficient disincentive for people to break the law. That is why I ask the Minister again to consider reviewing the clause and to ask herself, her officials and her Government colleagues whether we should consider a sanction of a custodial sentence where people get in the way of an investigation by the Information Commissioner’s Office.

I am afraid that such activities will continue. I very much hope that the Secretary of State for Digital, Culture, Media and Sport reflects on our exchange on the Floor of the House this morning and uses the information he has about public contracts to do a little more work to expose who is in the network of individuals associated with Cambridge Analytica and where other companies may be implicated in this scandal. We know, because it has said so, that Cambridge Analytica is in effect a shell company—it is in effect a wholly owned subsidiary of SCL Elections Ltd—but we also know that it has an intellectual property sharing agreement with other companies, such as AggregateIQ. Mr Alexander Nix, because he signed the non-disclosure agreement, was aware of that. There are relationships between companies around Cambridge Analytica that extend far and wide. I mentioned this morning that I am concerned that the Foreign and Commonwealth Office may be bringing some of them together for its computational propaganda conference somewhere in the countryside this weekend.

The point I really want the Minister to address is whether she is absolutely content that the sanctions proposed under the clause are sufficient to deter and prosecute the kind of misbehaviour, albeit still only alleged, that has been in the news this week, which raises real concerns.

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): I will be very brief, because I will largely echo what the right hon. Member for Birmingham, Hodge Hill said. It is absolutely fair to say that our understanding of the potential value of personal information, including that gained by people who break data protection laws, has increased exponentially in recent times, as has our understanding of the damage that can be done to victims of such breaches. I agree that it is not easy to see why the proposed offences stop where they do.

I have a specific question about why there is a two-tier system of penalties. There is a set of offences that are triable only in a summary court and for which there is a maximum fine. I think the maximum in Scotland and Northern Ireland is £5,000. There is a second set of offences that could conceivably be triable on indictment, and there is provision there for an unlimited fine, but not any custodial sentence.

For some companies, if they were in trouble, a £5,000 fine for essentially obstructing justice would be small beer, especially if it allowed them to avoid an unlimited fine. It would be interesting to hear an explanation for that. Many folk would see some of the offences that are triable on indictment as morally equivalent to embezzlement, serious theft or serious fraud, so it is legitimate to ask why there is no option for a custodial sentence in any circumstance.

Margot James: I certainly share the concerns that hon. Members have expressed in the light of the dreadful Cambridge Analytica scandal. I will set out the penalties for summary only offences, which lie in clause 119, “Inspection of personal data in accordance with international obligations”; clause 173, “Alteration etc of personal data to prevent disclosure”; and paragraph 15(1) of schedule 15, which contains the offence of obstructing the execution of a warrant. The maximum penalty on summary conviction for those offences is an unlimited fine in England and Wales or a level 5 fine in Scotland and Northern Ireland.

Clause 189(2) sets out the maximum penalties for offences that can be tried summarily on indictment, which include offences in clause 132 “Confidentiality of information”; clause 145 “False statements made in response to an information notice”; clause 170 “Unlawful obtaining etc of personal data”; clause 171 “Re-identification of de-identified personal data”; and clause 181 “Prohibition of requirement to produce relevant records”. Again, the maximum penalty when tried summarily in England or Wales, or on indictment, is an unlimited fine. In Scotland and Northern Ireland, the maximum penalty on summary conviction is a fine “not exceeding the statutory maximum” of an unlimited fine when tried on indictment.

Liam Byrne: I was listening carefully to the Minister’s reply. She said that the sanction is an unlimited fine in England and Wales. Let us take the hypothetical case of Cambridge Analytica, which is a one-man shell company, in effect; in the UK, it is wholly owned by SCL Elections. I am concerned about what happens if that holding company—let us say it is SCL Elections—is registered outside England and Wales, in the United States or Uruguay, for example? Will the fine bite on the one-man shell company, Cambridge Analytica? If so, the shell company will just go out of business—the directors will be struck off and that will be the end of it. That is not much of a sanction.

Margot James: The sanctions are as I outlined. The right hon. Gentleman talks about more complex corporate structures. Later in our proceedings, we will touch on the jurisdiction of the general data protection regulation when it comes to dealing with cross-border situations outside the European Union. Perhaps we can throw some light on what he is saying when we come to that point.

The GDPR strengthens the rights of data subjects over their data, including the important right of consent and what constitutes consent by the data subject to the use and processing of their data. That right must now be clear, robust and unambiguous. That is a key change that will provide some protection in the future.

The right hon. Gentleman should remember that, in addition to data protection laws, other sanctions are available, including prosecution for computer misuse, fraud and, potentially, in the case of the example we have been talking about, electoral laws, depending on the circumstances.

Question put and agreed to.

Clause 189 accordingly ordered to stand part of the Bill.

Clause 190 ordered to stand part of the Bill.
Clause 191

LIABILITY OF DIRECTORS ETC

Question proposed, That the clause stand part of the Bill.

12 noon

Liam Byrne: The debate presents what is potentially a good opportunity to offer a flow of advice to the Minister, if I might pose my question like this: if a company based in the UK has committed an offence, but its holding company is based somewhere else, in what way will clause 191 bite not on the UK operations, but on the holding company elsewhere?

My reading of the extraterritoriality provisions is that the implementation of GDPR and the sanctions around it may well bite in Europe—we will get on to this issue in the debate on extraterritoriality, as the Minister has said—but where companies are registered in, heaven forbid, various tax havens around the world such as Panama or Belize, will the Information Commissioner be able to, in effect, bring prosecutions that will result in action biting on a director of a holding company domiciled somewhere abroad, such as Belize? That is a pretty plausible scenario. Again, this touches on whether the sanctions in the Bill are sufficient to deter the kind of misbehaviour that we now know is running loose around the world that the Secretary of State described.

Margot James: The clause allows proceedings to be brought against a director, or a person acting in a similar position, as well as the body corporate, where it has been proven that breaches of the Act have occurred with the consent, connivance or negligence of that person. The clause will have the same effect as that of section 61 of the Data Protection Act 1998. I might have to come back to the right hon. Gentleman on some of the points he raised in that hypothetical circumstance, which I have no doubt could certainly exist in the future.

Liam Byrne: I would be grateful if the Minister wrote to me on that this afternoon, because if there are deficiencies we will have to get on with preparing amendments for consideration on Report.

Question put and agreed to.

Clause 191 accordingly ordered to stand part of the Bill.

Clauses 192 to 195 ordered to stand part of the Bill.

Clause 196

TRIBUNAL PROCEDURE RULES

Question proposed, That the clause stand part of the Bill.

Liam Byrne: Questions have arisen on the procedure rules associated with tribunals. The Opposition are concerned that the rights conferred in the Bill are rights in reality, not in theory. That is why we moved important amendments earlier, which were unwisely rejected by the Government, on collective forms of class action.

If we are to ensure that our constituents genuinely have access to the kind of justice mechanisms set out in the clause, we are obviously required to confront the reality that people will sometimes not have the resources for the financing of solicitors or representatives to help them to make their cases. Will the Minister say a word about whether our constituents will have access to resources such as legal aid to fight those cases in a tribunal?

Margot James: The clause provides a power to make tribunal procedure rules to regulate how the rights of appeal before the tribunal and the right to apply for an order from the tribunal, conferred under the Bill, are exercised. It sets out the way a data subject’s right to authorise a representative body to apply for an order on his or her behalf under article 80 of the GDPR and clause 183 can be exercised. For somebody who does not have the means to pursue an individual claim, that is obviously a way forward in some circumstances. In addition, it provides a power to make provision about “securing the production of material used for the processing of personal data,”

and

“the inspection, examination, operation and testing of equipment or material used in connection with the processing of personal data.”

The provisions are equivalent to paragraph 7 of schedule 6 of the 1998 Act.

Liam Byrne: That is a helpful explanation. It is obvious from the Minister’s response that those tribunal rules will be incredibly important in providing democratic access to justice where our constituents have been maligned and their data rights abused. The tribunal procedure rules, given what she has said, will be of great interest to right hon. and hon. Members.

Will the Minister clarify what oversight and scrutiny we may have in the House of those tribunal procedure rules, or whether they are purely rules that are the child of the tribunal authorities? Are they something the tribunal authorities can just issue, or is there some oversight, amendment or improvement that we in the House can provide?

Margot James: I cannot be precise about the level of scrutiny that the tribunal procedure rules may or may not be subject to, but in further answer to the right hon. Gentleman’s earlier question, legal aid is also available, as set out in the Legal Aid, Sentencing and Punishment of Offenders Act 2012, where a failure to fund would breach the European convention on human rights. There is that protection over and above the right of people to join a group action. The rules set by the Tribunal Procedure Rules Committee will be set, I am told, by applying its own consultation process, which the Lord Chancellor lays before Parliament.

Question put and agreed to.

Clause 196 accordingly ordered to stand part of the Bill.

Clause 197 ordered to stand part of the Bill.

Clause 198

OTHER DEFINITIONS

Amendments made: 70, in clause 198, page 114, line 25, at end insert
“the following (except in the expression “United Kingdom government department”)

This amendment makes clear that the definition of “government department” does not operate on references to a “United Kingdom government department” (which can be found in Clause 185 and paragraph 1 of Schedule 7).
Amendment 71, in clause 198, page 115, line 8, at end insert—

“(2) References in this Act to a period expressed in hours, days, weeks, months and years, except in—

(a) section 125(4), (7) and (8);
(b) section 160(3), (5) and (6);
(c) section 176(2);
(d) section 179(8) and (9);
(e) section 180(4);
(f) section 186(3), (5) and (6);
(g) section 190(3) and (4);
(h) paragraph 18(4) and (5) of Schedule 1;
(i) paragraphs 5(4) and 6(4) of Schedule 3;
(j) Schedule 4;
(k) paragraph 11(5) of Schedule 12;
(l) Schedule 15;

(and the references in section 5 to terms used in Chapter 2 or 3 of Part 2 do not include references to a period expressed in hours, days, weeks, months or years).”

This amendment provides that periods of time referred to in the bill are generally to be interpreted in accordance with Article 3 of Regulation 1182/71, which makes provision about the calculation of periods of hours, days, weeks, months and years.

Amendment 182, in clause 198, page 115, line 8, at end insert—

“( ) Section 3(14)(aa) (interpretation of references to Chapter 2 of Part 2 in Parts 5 to 7) and the amendments in Schedule 18 which make equivalent provision are not to be treated as implying a contrary intention for the purposes of section 20(2) of the Interpretation Act 1978, or any similar provision in another enactment, as it applies to other references to, or to a provision of, Chapter 2 of Part 2 of this Act.”

—(Margot James.)

Clause 198, as amended, ordered to stand part of the Bill.

Clause 199 ordered to stand part of the Bill.

Clause 200

TERRITORIAL APPLICATION OF THIS ACT

Amendments made: 183, in clause 200, page 117, line 15, leave out subsections (1) to (4) and insert—

“(1) This Act applies only to processing of personal data described in subsections (2) and (3).

(2) It applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the United Kingdom, whether or not the processing takes place in the United Kingdom.

(3) It also applies to the processing of personal data to which Chapter 2 of Part 2 (the GDPR) applies where—

(a) the processing is carried out in the context of the activities of an establishment of a controller or processor in a country or territory that is not a member State, whether or not the processing takes place in such a country or territory,

(b) the personal data relates to a data subject who is in the United Kingdom when the processing takes place, and

(c) the processing activities are related to—

(i) the offering of goods or services to data subjects in the United Kingdom, whether or not for payment, or

(ii) the monitoring of data subjects’ behaviour in the United Kingdom.’

This amendment replaces the existing provision on territorial application in clause 200(1) to (4). In the amendment, subsection (2) provides that the bill applies to processing in the context of the activities of an establishment of a controller or processor in the UK. Subsection (3) provides that, in certain circumstances, the bill also applies to processing to which the GDPR applies and which is carried out in the context of activities of an establishment of a controller or processor in a country or territory that is not part of the EU.

Amendment 184, in clause 200, page 118, line 8, leave out “(4)” and insert “(3)”.

This amendment is consequential on amendment 183.

Amendment 185, in clause 200, page 118, leave out line 10 and insert “processing of personal data”.

This amendment is consequential on amendment 183.

Amendment 186, in clause 200, page 118, line 10, at end insert—

‘(5A) Section 3(14)(b) does not apply to the reference to the processing of personal data in subsection (2).

(5B) The reference in subsection (3) to Chapter 2 of Part 2 (the GDPR) does not include that Chapter as applied by Chapter 3 of Part 2 (the applied GDPR).’

New subsection (5A) secures that the reference to “processing” in the new subsection (2) inserted by amendment 183 includes all types of processing of personal data. It disapplies clause 3(14)(b), which provides that references to processing in Parts 5 to 7 of the bill are usually only to processing to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies. New subsection (5B) ensures that the reference in the new subsection (3) to Chapter 2 of Part 2 of the bill does not include that Chapter as applied by Chapter 3 of Part 2.

Amendment 187, in clause 200, page 118, line 11, leave out “established” and insert “who has an establishment”.

This amendment is consequential on amendment 183.

Amendment 188, in clause 200, page 118, line 21, after “to” insert “a person who has an”.

This amendment is consequential on amendment 183.

Amendment 189, in clause 200, page 118, line 23, leave out subsection (7).—(Margot James.)

This amendment is consequential on amendment 183.

Question proposed, That the clause, as amended, stand part of the Bill.

Liam Byrne: This is where we get into some of the whys and wherefores of the territorial application of the Bill. We can see in clause 200(1) that the Bill essentially bites on a data controller who is domiciled here in the United Kingdom. A question of public concern—it should also concern us in this Committee—is whether the bite and sanctions of the Bill will touch on people who are registered here, but not necessarily on directors of holding companies who are domiciled elsewhere.

I expect that the things we will learn about over the weekend and into next week will confirm for us all that very small companies—essentially corporate shells—that are perhaps registered as data controllers and might have committed offences under the 1998 Act or under the Bill, once it has received Royal Assent, might be controlled by directors who are domiciled elsewhere. If the Bill is to be worth anything and if it is to change
[Liam Byrne]

anything in the real world in which we happen to live, there is a real question about how offences committed under it by people here will be limited by the corporate realities, which mean that shell companies are data controllers, but actually the wealth, assets and operating mind of a company are somewhere else. Perhaps the Minister will say a little about how she will tackle that particular problem, because we know it is going to arise.

Margot James: First, a word on the clause, which sets out the territorial application with respect to the circumstances in which the Bill applies to the processing of personal data. Article 3 of the GDPR says that the GDPR applies where the processing of personal data occurs in the context of the activities of a controller or a processor established in the EU, and that it will also apply where a controller or processor is based outside the EU, but is processing the data of people within the EU in connection with the offering of goods and services to them, or for monitoring their behaviour.

We have revisited the clause to ensure that, as far as possible, the scope of the Bill aligns with the scope of the GDPR, albeit in a UK-only context. The Bill will allow the sanction to be given to an overseas entity where it is in the control of a UK-based company. Whether it can be enforced will depend on international arrangements for bringing people to justice, including those beyond the area of data protection.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

Whether it can be enforced will depend on international arrangements for bringing people to justice, including those beyond the area of data protection.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.

One additional point, regarding the global nature of these crimes, is that under UK law we already have stronger data protection laws than many other countries—indeed, considerably stronger than in the United States. That means that American citizens with an interest in these crimes, which are of course strengthening through the Bill.
Amendment 192, in schedule 18, page 210, line 4, at end insert—

"Pharmacy (Northern Ireland) Order 1976 (S.I. 1976/1213 (N.I. 22))"

8A The Pharmacy (Northern Ireland) Order 1976 is amended as follows.

8B In article 2(2) (interpretation), omit the definition of “Directive 95/46/EC”.

8C In article 8D (European professional card), after paragraph (3) insert—

“(4) In Schedule 2C, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018;”.

8D In article 22A(6) (Directive 2005/36/EC: functions of competent authority etc.), before sub-paragraph (a) insert—

“(za) “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018;”.

8E(1) Schedule 2C (Directive 2005/36/EC: European professional card) is amended as follows.

(2) In paragraph 8(1) (access to data), for “Directive 95/46/EC” substitute “the GDPR”.

(3) In paragraph 9 (processing data), omit sub-paragraph (2) (deeming the Society to be the controller for the purposes of Directive 95/46/EC).

8F (1) The Table in Schedule 2D (functions of the Society under Directive 2005/36/EC) is amended as follows.

(2) In the entry for Article 56(2), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

(3) In the entry for Article 56a(4), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

8G (1) Paragraph 2 of Schedule 3 (fitness to practice: disclosure of information) is amended as follows.

(2) In sub-paragraph (2)(a), after “provision” insert “or the GDPR”.

(3) For sub-paragraph (3) substitute—

“(3) In determining for the purposes of sub-paragraph (2)(a) whether a disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this section.”

(4) After sub-paragraph (4) insert—

“(5) In this paragraph, “the GDPR” and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(10), (11) and (14) of that Act).”

Representation of the People Act 1983 (c. 2)

8H (1) Schedule 2 to the Representation of the People Act 1983 (provisions which may be contained in regulations as to registration etc) is amended as follows.

(2) In paragraph 1A(5), for “the Data Protection Act 1998” substitute “Parts 5 to 7 of the Data Protection Act 2018 (see section 3(4) and (14) of that Act)”.

(3) In paragraph 8C(2), for “the Data Protection Act 1998” substitute “Parts 5 to 7 of the Data Protection Act 2018 (see section 3(4) and (14) of that Act)”.

(4) In paragraph 1A—

(a) in sub-paragraph (1) for “who are data users to supply data, or documents containing information extracted from data and” substitute “to supply information”, and

(b) omit sub-paragraph (2).”

This amendment makes consequential amendments to primary legislation.

Amendment 193, in schedule 18, page 210, leave out lines 5 to 39 and insert—

“Medical Act 1983 (c. 54)”

9 The Medical Act 1983 is amended as follows.

10 (1) Section 29E (evidence) is amended as follows.

(2) In subsection (5), after “enactment” insert “or the GDPR”.

(3) For subsection (7) substitute—

“(7) In determining for the purposes of subsection (5) whether a disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this section.”

(4) In subsection (9), at the end insert—

“the GDPR” and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(10), (11) and (14) of that Act).”

11 (1) Section 35A (General Medical Council’s power to require disclosure of information) is amended as follows.

(2) In subsection (4), after “enactment” insert “or the GDPR”.

(3) For subsection (5A) substitute—

“(5A) In determining for the purposes of subsection (4) whether a disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and Schedule 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this section.”

(4) In subsection (7), at the end insert—

“the GDPR” and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(10), (11) and (14) of that Act).”

12 In section 49B(7) (Directive 2005/36: designation of competent authority etc.), after “Schedule 4A” insert—

“the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018;”.

13 In section 55(1) (interpretation), omit the definition of “Directive 95/46/EC”.

13A (1) Paragraph 9B of Schedule 1 (incidental powers of the General Medical Council) is amended as follows.

(2) In sub-paragraph (2)(a), after “enactment” insert “or the GDPR”.

(3) After sub-paragraph (3) insert—

“(4) In this paragraph, “the GDPR” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(10), (11) and (14) of that Act).”
13B (1) Paragraph 5A of Schedule 4 (professional performance assessments and health assessments) is amended as follows.

(2) In sub-paragraph (8), after “enactment” insert “or the GDPR”.

(3) For sub-paragraph (8A) substitute—

“(8A) In determining for the purposes of sub-paragraph (8) whether a disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this paragraph.”

(4) After sub-paragraph (13) insert—

“(14) In this paragraph, “the GDPR” and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(10), (11) and (14) of that Act).”

13C (1) The table in Schedule 4A (functions of the General Medical Council as competent authority under Directive 2005/36) is amended as follows.

(2) In the entry for Article 56(2), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

(3) In the entry for Article 56a(4), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

This amendment replaces the existing consequential amendments of the Medical Act 1983.

Amendment 194, in schedule 18, page 211, line 18, leave out from “GDPR” to “(see” in line 19 and insert “and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act”.

This amendment makes clear that in section 33B of the Dentists Act 1984 references to Schedule 2 to the bill include that Schedule as applied by Chapter 3 of Part 2 of the bill.

Amendment 195, in schedule 18, page 211, line 20, at end insert—

15A In section 36ZA(6) (Directive 2005/36: designation of competent authority etc), after “Schedule 4ZA—” insert—

“‘the GDPR’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018;”.

This amendment makes further consequential amendments to the Dentists Act 1984.

Amendment 196, in schedule 18, page 211, line 39, leave out from “GDPR” to “(see” in line 40 and insert “and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act”.

This amendment makes clear that in section 36Y of the Dentists Act 1984 references to Schedule 2 to the bill include that Schedule as applied by Chapter 3 of Part 2 of the bill.

Amendment 197, in schedule 18, page 211, line 41, at end insert—

16A In section 53(1) (interpretation), omit the definition of “Directive 95/46/EC”.


(2) In the entry for Article 56(2), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

(3) In the entry for Article 56a(4), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

Companies Act 1985 (c. 6)

16C In section 449(11) of the Companies Act 1985 (provision for security of information obtained), for “the Data Protection Act 1998” substitute “the data protection legislation”. “

This amendment makes consequential amendments to primary legislation, including further consequential amendments to the Dentists Act 1984.

Amendment 198, in schedule 18, page 212, line 16, leave out from “GDPR” to “(see” in line 17 and insert “and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act”.

This amendment makes clear that in section 13B of the Opticians Act 1989 references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act.

Amendment 199, in schedule 18, page 212, line 18, at end insert—


18B For section 2 substitute—

“2 Health professionals

In this Act, “health professional” has the same meaning as in the Data Protection Act 2018 (see section 197 of that Act).”

18C (1) Section 3 (right of access to health records) is amended as follows.

(2) In subsection (2), omit “Subject to subsection (4) below,”.

(3) In subsection (4), omit from “other than the following” to the end.

This amendment makes consequential amendments to the Access to Health Records Act 1990.

Amendment 200, in schedule 18, page 213, line 2, at end insert—


(2) In paragraph (3), for “the Data Protection Act 1998” substitute “the data protection legislation”.

(3) After paragraph (6) insert—

“(7) In this Article, “the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act).”

This amendment makes consequential amendments to the Industrial Relations (Northern Ireland) Order 1992.

Amendment 201, in schedule 18, page 215, line 10, leave out from “data” to “(see” in line 11 and insert “, “processing” and references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act”.

This amendment makes clear that in section 40 of the Freedom of Information Act 2000 references to a provision of Chapter 2 of Part 2 of the bill include that provision as applied by Chapter 3 of Part 2 of the bill.

Amendment 202, in schedule 18, page 215, line 15, leave out from “GDPR” to “(see” in line 16 and insert “and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act”.

This amendment makes clear that in section 7A of the Health and Personal Social Services Act (Northern Ireland) 2001 references to Schedule 2 to the bill include that Schedule as applied by Chapter 3 of Part 2 of the bill.

Amendment 203, in schedule 18, page 220, line 7, at end insert—
64A (1) Section 237 of the Enterprise Act 2002 (general restriction on disclosure) is amended as follows.

(2) In subsection (4), for “the Data Protection Act 1998 (c. 29)” substitute “the data protection legislation”.

(3) After subsection (6) insert—

“(7) In this section, “the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act).”

This amendment makes consequential amendments to the Enterprise Act 2002.

Amendment 204, in schedule 18, page 221, line 21, leave out from “data”” to “(see” in line 22 and insert “, “processing” and references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act”

This amendment makes clear that in section 38 of the Freedom of Information (Scotland) Act 2002 references to a provision of Chapter 2 of Part 2 of the bill include that provision as applied by Chapter 3 of Part 2 of the bill.

Amendment 205, in schedule 18, page 222, line 21, at end insert—

“(Mental Health (Care and Treatment) (Scotland) Act 2003 (asp 13)

75A (1) Section 279 of the Mental Health Care and Treatment (Scotland) Act 2003 (information for research) is amended as follows.

(2) In subsection (2), for “research purposes within the meaning given by section 33 of the Data Protection Act 1998 (c. 29) (research, history and statistics)” substitute “purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics)”.

(3) After subsection (9) insert—

“(10) In this section, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).”

This amendment makes consequential amendments to the Mental Health (Care and Treatment) (Scotland) Act 2003.

Amendment 206, in schedule 18, page 222, line 29, at end insert—

“(Companies (Audit, Investigations and Community Enterprise) Act 2004 (c. 27)

76A The Companies (Audit, Investigations and Community Enterprise) Act 2004 is amended as follows.

76B (1) Section 15A (disclosure of information by tax authorities) is amended as follows.

(2) In subsection (2)—

(a) omit “within the meaning of the Data Protection Act 1998”, and

(b) for “that Act” substitute “the data protection legislation”.

(3) After subsection (7) insert—

“(8) In this section—

“the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);

“personal data” has the same meaning as in Parts 5 to 7 of that Act (see section 3 of that Act).”

76C (1) Section 15D (permitted disclosure of information obtained under compulsory powers) is amended as follows.

(2) In subsection (7), for “the Data Protection Act 1998” substitute “the data protection legislation”.

(3) After subsection (7) insert—

“(8) In this section, “the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act).”

This amendment makes consequences to the Companies (Audit, Investigations and Community Enterprise) Act 2004.

Amendment 207, in schedule 18, page 225, line 10, at end insert—

85A (1) Section 264C (provision and disclosure of information about health service products: supplementary) is amended as follows.

(2) In subsection (2), for “the Data Protection Act 1998” substitute “the data protection legislation”.

(3) After subsection (3) insert—

(4) In this section, “the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act).”

This amendment makes further consequential amendments to the National Health Service Act 2006.

Amendment 208, in schedule 18, page 225, line 28 at end insert—

“(Companies Act 2006 (c. 46)

92A The Companies Act 2006 is amended as follows.

92B In section 458(2) (disclosure of information by tax authorities)—

(a) for “within the meaning of the Data Protection Act 1998 (c. 29)” substitute “within the meaning of Parts 5 to 7 of the Data Protection Act 2018 (see section 3 of that Act)”;

(b) for “that Act” substitute “the data protection legislation”.

92C In section 461(7) (permitted disclosure of information obtained under compulsory powers), for “the Data Protection Act 1998 (c. 29)” substitute “the data protection legislation”.

92D In section 948(9) (restrictions on disclosure) for “the Data Protection Act 1998 (c. 29)” substitute “the data protection legislation”.

92E In section 1173(1) (minor definitions: general), at the appropriate place insert—

“the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);”

92F In section 1224A(7) (restrictions on disclosure), for “the Data Protection Act 1998” substitute “the data protection legislation”.

92G In section 1253D(3) (restriction on transfer of audit working papers to third countries), for “the Data Protection Act 1998” substitute “the data protection legislation”.

92H In section 1261(1) (minor definitions: Part 42), at the appropriate place insert—

“the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);”

92I In section 1262 (index of defined expressions: Part 42), at the appropriate place insert—

the data protection legislation section 1261(1).”

92J In Schedule 8 (index of defined expressions: general), at the appropriate place insert—

the data protection legislation section 1173(1).”

This amendment makes consequential amendments to the Companies Act 2006.

Amendment 209, in schedule 18, page 225, line 38, at end insert—

96A (1) Section 45 (information held by HMRC) is amended as follows.

(2) In subsection (4A), for “section 51(3) of the Data Protection Act 1998” substitute “section 128 of the Data Protection Act 2018”.

(3) In subsection (4B), for “the Data Protection Act 1998” substitute “the Data Protection Act 2018”.

This amendment makes further consequential amendments to the Statistics and Registration Service Act 2007.
Amendment 210, in schedule 18, page 230, line 16, at end insert—

"Coroners and Justice Act 2009 (c. 25)
122A In Schedule 21 of the Coroners and Justice Act 2009 (minor and consequential amendments), omit paragraph 29(3)."

This amendment makes a consequential amendment to the Coroners and Justice Act 2009 and is consequential on the amendments being made to section 3 of the Access to Health Records Act 1990 by amendment 199.

Amendment 211, in schedule 18, page 232, line 39, after “after “”, insert “this”

Paragraph 130(3) of Schedule 18 to the bill amends paragraph 8(8) of Schedule 2 to the Welsh Language (Wales) Measure 2011 by inserting new text. This amendment clarifies where that new text is to be inserted in the English language version of that Measure.

Amendment 212, in schedule 18, page 242, line 40, at end insert—

"Additional Learning Needs and Educational Tribunal (Wales) Act 2018 (anaw 2)
186A (1) Section 4 of the Additional Learning Needs and Educational Tribunal (Wales) Act 2018 (additional learning needs code) is amended as follows.

(2) In the English language text—
(a) in subsection (9), omit from “and in this subsection” to the end, and
(b) after subsection (9) insert—

“(9A) In subsection (9)—
“data subject” (“testun y data”) has the meaning given by section 3(5) of the Data Protection Act 2018;
“personal data” (“data personol”) has the same meaning as in Parts 5 to 7 of that Act (section 3(2) and (14) of that Act).

(3) In the Welsh language text—
(a) in subsection (9), omit from “ac yn yr is-adran hon” to the end, and
(b) after subsection (9) insert—

“(9A) Yn is-adran (9)—
mae i “data personol” yr un ystyr ag a roddir i “personal data” yn Rhanau 5 i 7 o Ddeddf Diogelu Data 2018 (gweler adran 3(2) a (14) o Ddeddf honno);
mae i “testun y data” yr ystyr a roddir i “data subject” gan adran 3(5) o Ddeddf honno.”

This amendment makes consequential amendments to the Additional Learning Needs and Educational Tribunal (Wales) Act 2018.

Amendment 213, in schedule 18, page 243, line 14, at end insert—

"Estate Agents (Specific Offences) (No. 2) Order 1991 (S.I. 1991/1091)
187A In the table in the Schedule to the Estate Agents (Specified Offences) (No. 2) Order 1991 (specified offences), at the end insert—

“Data Protection Section 145 False statements made in response to an information notice.”

This amendment makes a consequential amendment to the Estate Agents (Specific Offences) (No. 2) Order 1991.

Amendment 214, in schedule 18, page 243, line 22, after “controller.,” insert—

(ba) after “in the context of” insert “the activities of.”

This amendment to the consequential amendment to the Channel Tunnel (International Agreements) Order 1993 is consequential on amendment 183.

Amendment 215, in schedule 18, page 243, line 27, after “controller.,” insert—

(ba) after “in the context of” insert “the activities of.”

This amendment to the consequential amendment to the Channel Tunnel (International Agreements) Order 1993 is consequential on amendment 183.

Amendment 216, in schedule 18, page 243, line 28, at end insert—

188A The Access to Health Records (Northern Ireland) Order 1993 is amended as follows.

188B In Article 4 (health professionals), for paragraph (1) substitute—

“(1) In this Order, “health professional” has the same meaning as in the Data Protection Act 2018 (see section 197 of that Act).”

188C In Article 56a(a) (fees for access to health records), for “under section 7 of the Data Protection Act 1998” substitute “made by the Department”.

188D In article 4 of the Channel Tunnel (Miscellaneous Provisions) Order 1994 (application of enactments), for paragraphs (2) and (3) substitute—

“(2) For the purposes of section 200 of the Data Protection Act 2018 (“the 2018 Act”), data which is processed in a control zone in Belgium, in connection with the carrying out of frontier controls, by an officer belonging to the United Kingdom is to be treated as processed by a controller established in the United Kingdom in the context of the activities of that establishment (and accordingly the 2018 Act applies in respect of such data).

(3) For the purposes of section 200 of the 2018 Act, data which is processed in a control zone in Belgium, in connection with the carrying out of frontier controls, by an officer belonging to the Kingdom of Belgium is to be treated as processed by a controller established in the Kingdom of Belgium in the context of the activities of that establishment (and accordingly the 2018 Act does not apply in respect of such data)."

European Primary and Specialist Dental Qualifications Regulations 1998 (S.I. 1998/811)
188E The European Primary and Specialist Dental Qualifications Regulations 1998 are amended as follows.

188F (1) Regulation 2(1) (interpretation) is amended as follows.

(2) Omit the definition of “Directive 95/46/EC”.

(3) At the appropriate place insert—

““the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018;”.

188G (1) The table in Schedule A1 (functions of the GDC under Directive 2005/36) is amended as follows.

(2) In the entry for Article 56(2), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

(3) In the entry for Article 56a(4), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

188H For article 7 of the Scottish Parliamentary Corporate Body (Crown Status) Order 1999 substitute—

“7 Data Protection Act 2018
(1) The Parliamentary corporation is to be treated as a Crown body for the purposes of the Data Protection Act 2018 to the extent specified in this article.

(2) The Parliamentary corporation is to be treated as a government department for the purposes of the following provisions—
(a) section 8(d) (lawfulness of processing under the GDPR: public interest etc),
(b) section 202 (application to the Crown),
188I For article 9 of the Northern Ireland Assembly Commission (Crown Status) Order 1999 in Parts 5 to 7 of that Act (see section 3(14) of that Act).”

Part 2 of the Data Protection Act 2018 have the same meaning as

insert—

188K In regulation 3(1) (interpretation), at the appropriate places (S.I. 2001/341)

Representation of the People (England and Wales) Regulations 2001 (S.I. 1999/3145)

188M For article 9 of the Northern Ireland Assembly Commission (Crown Status) Order 1999 substitute—

9 Data Protection Act 2018

(1) The Commission is to be treated as a Crown body for the purposes of the Data Protection Act 2018 to the extent specified in this article.

(2) The Commission is to be treated as a government department for the purposes of the following provisions—

(a) section24(3) (exemption for certain data relating to employment under the Crown),

(b) section202(6) (application of certain provisions to a person in the service of the Crown).

(5) In this article, references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(14) of that Act).”
Northern Ireland Assembly Commission (Crown Status) Order 1999

188T In regulation 99(6) and (7) (supply of free copy of full register in respect of name under section10ZD), for “the Data Protection Act 1998” substitute “the data protection legislation”. 188U In regulation 109A(9) and (10) (supply of free copy of full register to public libraries and local authority archives services and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 188V In regulation 119(2) (conditions on the use, supply and disclosure of documents open to public inspection), for sub-paragraph (i) (but not the final “or”) substitute—

(a) Article 89 GDPR purposes;”.

188W The Representation of the People (Scotland) Regulations 2001 (S.I. 2001/497)

188X In regulation 3(1) (interpretation), at the appropriate places

insert—

“Article 89 GDPR purposes” means the purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”;

“the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);”;

“the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);”.

188L In regulation 26(3)(a) (applications for registration), for “the Data Protection Act 1998” substitute “the data protection legislation”.

188M In regulation 26A(2)(a) (application for alteration of register in respect of name under section 10ZD), for “the Data Protection Act 1998” substitute “the data protection legislation”.

188N In regulation 32ZA(3)(f) (annual canvass), for “the Data Protection Act 1998” substitute “the data protection legislation”.

188O In regulation 61A (conditions on the use, supply and inspection of absent voter records or lists), for paragraph (a) (but not the final “or”) substitute—

(a) Article 89 GDPR purposes;”.

188P (1) Regulation 92(2) (interpretation and application of Part VI etc) is amended as follows.

(2) After sub-paragraph (b) insert—

“(ba) “relevant requirement” means the requirement under Article 89 of the GDPR, read with section 19 of the Data Protection Act 2018, that personal data processed for Article 89 GDPR purposes must be subject to appropriate safeguards.”

(3) Omit sub-paragraphs (c) and (d).

188Q In regulation 96(2A)(b)(i) (restriction on use of the full register), for “section 11(3) of the Data Protection Act 1998” substitute “section 123(5) of the Data Protection Act 2018”.

188R In regulation 97(5) and (6) (supply of free copy of full register to the British Library and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 188S In regulation 97A(7) and (8) (supply of free copy of full register to the National Library of Wales and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 188T In regulation 99(6) and (7) (supply of free copy of full register to Statistics Board and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 188U In regulation 109A(9) and (10) (supply of free copy of full register to public libraries and local authority archives services and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”.

188V In regulation 119(2) (conditions on the use, supply and disclosure of documents open to public inspection), for sub-paragraph (i) (but not the final “or”) substitute—

(i) Article 89 GDPR purposes;”.

188W The Representation of the People (Scotland) Regulations 2001 (S.I. 2001/497)

188X In regulation 3(1) (interpretation), at the appropriate places

insert—

“Article 89 GDPR purposes” means the purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”;

“the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);”;

“the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);”.

“...the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);”.

188L In regulation 26(3)(a) (applications for registration), for “the Data Protection Act 1998” substitute “the data protection legislation”.

188M In regulation 26A(2)(a) (application for alteration of register in respect of name under section 10ZD), for “the Data Protection Act 1998” substitute “the data protection legislation”.

188N In regulation 32ZA(3)(f) (annual canvass), for “the Data Protection Act 1998” substitute “the data protection legislation”.

188O In regulation 61A (conditions on the use, supply and inspection of absent voter records or lists), for paragraph (a) (but not the final “or”) substitute—

(a) Article 89 GDPR purposes;”.

188P (1) Regulation 92(2) (interpretation and application of Part VI etc) is amended as follows.

(2) After sub-paragraph (b) insert—

“(ba) “relevant requirement” means the requirement under Article 89 of the GDPR, read with section 19 of the Data Protection Act 2018, that personal data processed for Article 89 GDPR purposes must be subject to appropriate safeguards.”

(3) Omit sub-paragraphs (c) and (d).

188Q In regulation 96(2A)(b)(i) (restriction on use of the full register), for “section 11(3) of the Data Protection Act 1998” substitute “section 123(5) of the Data Protection Act 2018”.

188R In regulation 97(5) and (6) (supply of free copy of full register to the British Library and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 188S In regulation 97A(7) and (8) (supply of free copy of full register to the National Library of Wales and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 188T In regulation 99(6) and (7) (supply of free copy of full register to Statistics Board and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 188U In regulation 109A(9) and (10) (supply of free copy of full register to public libraries and local authority archives services and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 188V In regulation 119(2) (conditions on the use, supply and disclosure of documents open to public inspection), for sub-paragraph (i) (but not the final “or”) substitute—

(i) Article 89 GDPR purposes;”.

Representation of the People (Scotland) Regulations 2001 (S.I. 2001/497)

188W The Representation of the People (Scotland) Regulations 2001 are amended as follows.

188X In regulation 3(1) (interpretation), at the appropriate places

insert—

“Article 89 GDPR purposes” means the purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”;

“the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);”;

“the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);”.

“...the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);”. Continue...
188Y In regulation 26(3)(a) (applications for registration), for “the Data Protection Act 1998” substitute “the data protection legislation”.

188Z In regulation 26AC(2)(a) (application for alteration of register in respect of name under section 10(2D)), for “the Data Protection Act 1998” substitute “the data protection legislation”.

188AA In regulation 322A(3)(f) (annual canvass), for “the Data Protection Act 1998” substitute “the data protection legislation”.

188AB In regulation 61(3) (records and lists kept under Schedule 4), for paragraph (a) (but not the final “or”) substitute—

(a) Article 89 GDPR purposes;*

188AC In regulation 61A (conditions on the use, supply and inspection of absent voter records or lists), for paragraph (a) (but not the final “or”) substitute—

(a) Article 89 GDPR purposes;*

188AD (1) Regulation 92(2) (interpretation of Part VI etc) is amended as follows.

(2) After sub-paragraph (b) insert—

“(ba) “relevant requirement” means the requirement under Article 89 of the GDPR, read with section 19 of the Data Protection Act 2018, that personal data processed for Article 89 GDPR purposes must be subject to appropriate safeguards.”

(3) Omit sub-paragraphs (c) and (d).

188AE In regulation 95(3)(b)(i) (restriction on use of the full register), for “section 11(3) of the Data Protection Act 1998” substitute “section 123(5) of the Data Protection Act 2018”.

188AF In regulation 96(5) and (6) (supply of free copy of full register to the National Library of Scotland and the British Library and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”.

188AG In regulation 98(6) and (7) (supply of free copy of full register etc to Statistics Board and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”.

188AH In regulation 108A(9) and (10) (supply of full register to statutory library authorities and local authority archives services and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”.

188AI In regulation 119(2) (conditions on the use, supply and disclosure of documents open to public inspection), for sub-paragraph (i) (but not the final “or”) substitute—

(i) Article 89 GDPR purposes;*

Financial Services and Markets Act 2000 (Disclosure of Confidential Information) Regulations 2001 (S.I. 2001/2188)

188AJ (1) Article 9 of the Financial Services and Markets 2000 (Disclosure of Confidential Information) Regulations 2001 (disclosure by regulators or regulator workers to certain other persons) is amended as follows.

(2) In paragraph (2B), for sub-paragraph (a) substitute—

“(a) the disclosure is made in accordance with Chapter V of the GDPR”.

(3) Omit the definitions of “Data Protection Directive” and “Data Protection Regulation”, read with Chapter 2 of Part 2 of the Data Protection Act 2018 (see section 3(10), (11) and (14) of that Act).”

188AM (1) Article 25 (the Council’s power to require disclosure of information) is amended as follows.

(2) In paragraph (3), after “enactment” insert “or the GDPR”.

(3) In paragraph (6),

(a) for “paragraph (5),” substitute “paragraph (3)—”, and

(b) at the appropriate place insert—

“‘the GDPR’ has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(10), (11) and (14) of that Act).”

188AN In article 39B (European professional card), after paragraph (2) insert—

“(3) For the purposes of Schedule 2B, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018.”

188AO In article 40(6) (Directive 2005/36/EC: designation of competent authority etc), at the appropriate place insert—

“‘the GDPR’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018.”

188AP (1) Schedule 2B (Directive 2005/36/EC: European professional card) is amended as follows.

(2) In paragraph 8(1) (access to data) for “Directive 95/46/EC” substitute “the GDPR”.

(3) In paragraph 9 (processing data), omit sub-paragraph (2) (deeming the Society to be the controller for the purposes of Directive 95/46/EC).

188AQ (1) The table in Schedule 3 (functions of the Council under Directive 2005/36) is amended as follows.

(2) In the entry for Article 56(2), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

(3) In the entry for Article 56a(4), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.

188AR In Schedule 4 (interpretation), omit the definition of “Directive 95/46/EC”.


188AS Regulation 3 of the Electronic Commerce (EC Directive) Regulations 2002 (exclusions) is amended as follows.

188AT In paragraph (1)(b) for “the Data Protection Directive and the Telecommunications Data Protection Directive” substitute “the GDPR”.

188AU In paragraph (3)—

(a) omit the definitions of “Data Protection Directive” and “Telecommunications Data Protection Directive”, and

(b) at the appropriate place insert—

“‘the GDPR’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)’’.”

This amendment makes consequential amendments to secondary legislation, including to the Scottish Parliamentary Corporate Body (Crown Status) Order 1999 and the Northern Ireland Assembly Commission (Crown Status) Order 1999.

Amendment 217, in schedule 18, page 244, line 1, at end insert—

(d) for “data controller” substitute “controller”, and

(e) after “in the context of” insert “the activities of”. 
Amendment 218, in schedule 18, page 244, line 13, leave out from “GDPR” to “(see” in line 14 and insert “and references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act”.

This amendment makes clear that in the Environmental Information Regulations 2004 references to a provision of Chapter 2 of Part 2 of the bill include that provision as applied by Chapter 3 of Part 2 of the bill.

Amendment 219, in schedule 18, page 246, line 31, leave out from “GDPR” to “(see” in line 32 and insert “and references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act”.

This amendment makes clear that in the Environmental Information (Scotland) Regulations 2004 references to a provision of Chapter 2 of Part 2 of the bill include that provision as applied by Chapter 3 of Part 2 of the bill.

Amendment 220, in schedule 18, page 247, line 40, at end insert—


199A (1) Regulation 7 of the Licensing Act 2003 (Personal Licences) Regulations 2005 (application for grant of a personal licence) is amended as follows.

(2) In paragraph (1)(b)—

(a) for paragraph (iii)(but not the final “,” and”) substitute—

(iii) the results of a request made under Article 15 of the GDPR or section 45 of the Data Protection Act 2018 (rights of access by the data subject) to the National Identification Service for information contained in the Police National Computer”, and

(b) in the words following paragraph (iii), omit “search”.

(3) After paragraph (2) insert—

“(3) In this regulation, “the GDPR” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(10), (11) and (14) of that Act).”


199B The Education (Pupil Information) (England) Regulations 2005 are amended as follows.

199C In regulation 3(5) (meaning of educational record) for section 1(1) of the Data Protection Act 1998 substitute “section 3(4) of the Data Protection Act 2018”.

199D (1) Regulation 5 (disclosure of curricular and educational records) is amended as follows.

(2) In paragraph (4)—

(a) in sub-paragraph (a), for “the Data Protection Act 1998” substitute “the GDPR”, and

(b) in sub-paragraph (b), for “that Act or by virtue of any order made under section 30(2) or section 38(1) of the Act” substitute “the GDPR”.

(3) After paragraph (6) insert—

“(7) In this regulation, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018.”

This amendment makes consequential amendments to secondary legislation.

Amendment 221, in schedule 18, page 248, line 37, leave out from “GDPR” to “(see” in line 38 and insert “and references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act”.

This amendment makes clear that in regulation 45 of the Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 references to a provision of Chapter 2 of Part 2 of the bill include that provision as applied by Chapter 3 of Part 2 of the bill.
Amendment 222, in schedule 18, page 249, line 1, at end insert—

"Register of Judgments, Orders and Fines Regulations 2005 (S.I. 2005/3595)"

200A In regulation 3 of the Register of Judgments, Orders and Fines Regulations 2005 (interpretation)—

(a) for the definition of “data protection principles” substitute—

“‘data protection principles’ means the principles set out in Article 5(1) of the GDPR;”, and

(b) at the appropriate place insert—

“‘the GDPR’ has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section3(10), (11) and (14) of that Act);”.

Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 (S.S.I. 2005/494)

200B The Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005 are amended as follows.

(1) In paragraph 39 (sensitive information) is amended as follows.

(a) omit “sensitive personal data”, and

(b) substitute—

“personal data” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section3(2) and (14) of that Act).

(2) In determining for the purposes of this regulation whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article 6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted.

(3) Omit paragraphs (2) to (4).

National Assembly for Wales (Representation of the People) Order 2007 (S.I. 2007/236)

200D (1) Paragraph 14 of Schedule 1 to the National Assembly for Wales (Representation of the People) Order 2007 (absent voting at Assembly elections: conditions on the use, supply and inspection of absent vote records or lists) is amended as follows.

(2) The existing text becomes sub-paragraph (1).

(3) For paragraph (a) of that sub-paragraph (but not the final “or”) substitute—

(a) purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”.

(4) After that sub-paragraph insert—

“(2) In this paragraph, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).”


200E In regulation 3 of the Mental Capacity Act 2005 (Loss of Capacity during Research Project) (England) Regulations 2007 (research which may be carried out despite a participant’s loss of capacity), for paragraph (b) substitute—

“(b) any material used consists of or includes human cells or human DNA.”.


200F For article 5 of the National Assembly for Wales Commission (Crown Status) Order 2007 substitute—

“5 Data Protection Act 2018

(1) The Assembly Commission is to be treated as a Crown body for the purposes of the Data Protection Act 2018 to the extent specified in this article.

(2) The Assembly Commission is to be treated as a government department for the purposes of the following provisions—

(a) section 8(4) (lawfulness of processing under the GDPR: public interest etc),

(b) section202 (application to the Crown),

(c) paragraph 6 of Schedule1 (statutory etc and government purposes),

(d) paragraph 7 of Schedule2 (exemptions from the GDPR: functions designed to protect the public etc), and

(e) paragraph 8(1)(c) of Schedule3 (exemptions from the GDPR: health data).

(3) In the provisions mentioned in paragraph (4)—

(a) references to employment by or under the Crown are to be treated as including employment as a member of staff of the Assembly Commission, and

(b) references to a person in the service of the Crown are to be treated as including a person so employed.

(4) The provisions are—

(a) section24(3) (exemption for certain data relating to employment under the Crown), and

(b) section202(6) (application of certain provisions to a person in the service of the Crown).
(5) In this article, references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(14) of that Act).


200G In regulation 3 of the Mental Capacity Act 2005 (Loss of Capacity during Research Project) (Wales) Regulations 2007 (research which may be carried out despite a participant’s loss of capacity) —

(a) in the English language text, for paragraph (c) substitute—

“(c) any material used consists of or includes human cells or human DNA; and”,

and

(b) in the Welsh language text, for paragraph (c) substitute—

“(c) os yw unrhyw deunydd a defnyddir yn gellod ddynol neu’n DNA ddynol neu yn eu cynnwys; ac”.

Representation of the People (Absent Voting at Local Elections) (Scotland) Regulations 2007 (S.S.I. 2007/170)

200H (1) Regulation 18 of the Representation of the People (Absent Voting at Local Elections) (Scotland) Regulations 2007 (conditions on the use, supply and inspection of absent voter records or lists) is amended as follows.

(2) In paragraph (1), for sub-paragraph (a) (but not the final “or”) substitute—

“(a) purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”,

(3) After paragraph (1) insert—

“(2) In this regulation, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the freedom of movement of such data (General Data Protection Regulation).”

Representation of the People (Post-Local Government Elections Supply and Inspection of Documents) (Scotland) Regulations 2007 (S.S.I. 2007/264)

200I In regulation 5 of the Representation of the People (Post-Local Government Elections Supply and Inspection of Documents) (Scotland) Regulations 2007 (conditions on the use, supply and disclosure of documents open to public inspection)—

(a) in paragraph (2), for sub-paragraph (i) (but not the final “or”) substitute—

“(i) purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”,

and

(b) after paragraph (3) insert—

“(4) In this regulation, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the processing of personal data and on the free movement of such data (General Data Protection Regulation).”

Education (Pupil Records and Reporting) (Transitional) Regulations (Northern Ireland) 2007 (S.R. (N.I.) 2007 No. 43)

200K In regulation 2 (interpretation), at the appropriate place insert—

“the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data (General Data Protection Regulation),

Education (Pupil Records and Reporting) (Transitional) Regulations (Northern Ireland) 2007 is amended as follows.

200L In regulation 10(2) (duties of Boards of Governors), for “documents which are the subject of an order under section 30(2) of the Data Protection Act 1998” substitute “information to which the pupil to whom the information relates would have no right of access under the GDPR.”

Representation of the People (Northern Ireland) Regulations 2008 (S.I. 2008/1741)

200M In regulation 118 of the Representation of the People (Northern Ireland) Regulations 2008 (conditions on the use, supply and disclosure of documents open to public inspection)—

(a) in paragraph (2), for “research purposes within the meaning of that term in section 33 of the Data Protection Act 1998” substitute “purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics)”, and

(b) after paragraph (3) insert—

“(4) In this regulation, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data (General Data Protection Regulation).”


200N In paragraph 1(c) of the Schedule to the Companies Act 2006 (Extension of Takeover Panel Provisions) (Isle of Man) Order 2008 (modifications with which Chapter 1 of Part 28 of the Companies Act 2006 extends to the Isle of Man), for “the Data Protection Act 1998 (c 29)” substitute “the data protection legislation”.

Controlled Drugs (Supervision of Management and Use) (Wales) Regulations 2008 (S.I. 2008/3239 (W 286))

200O The Controlled Drugs (Supervision of Management and Use) (Wales) Regulations 2008 are amended as follows.

200P In regulation 2(1) (interpretation)—

(a) at the appropriate place in the English language text insert—

“the GDPR” ("y GDPR") and references to Schedule2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(10), (11) and (14) of that Act);”, and

(b) at the appropriate place in the Welsh language text insert—

“mæ i "y GDPR" a chyfreiriaidau at Atodlen2 i Ddeddf Diogelu Data 2018 yr un ystyr ag a roddir i “the GDPR” a chyfreiriaidau at yr Atodlen honno yn Rhannau 517 o'r Ddeddf honno (gweler adran 3(10), (11) a (14) o'r Ddeddf honno);”.

200Q (1) Regulation 25 (duty to co-operate by disclosing information as regards relevant persons) is amended as follows.

(2) In paragraph (7)—

(a) in the English language text, at the end insert “or the GDPR”,

and

(b) in the Welsh language text, at the end insert “neu’r GDPR”.

(3) For paragraph (8)—

(a) in the English language text substitute—

“(8) In determining for the purposes of paragraph (7) whether disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation; disclosures required by law) that the disclosure is required by this regulation.”,” and

(b) in the Welsh language text substitute—

“(8) Wth benderfynu at ddibenion paragraff (7) a yw datgeliad wedi’i wahardd, mae i’w dybied at ddibenion paragraff 5(2) o Atodlen 2 i Ddeddf Diogelu Data 2018 a pharagraff 3(2) o Atodlen 11 i Ddeddf honno (esemptiadau rhag darpariaeth penodol o’r ddeddfwriaeth diogelu data: datgeliadau sy’n olynol gan y gyfraith) bod y datgeliad wedi’i dyno am y rheoliad hwn.”

200R (1) Regulation 26 (responsible bodies requesting additional information be disclosed about relevant persons) is amended as follows.

(2) In paragraph (6)—
(a) in the English language text, at the end insert “or the GDPR”, and
(b) in the Welsh language text, at the end insert “neu’r GDPR”.

(3) For paragraph (7)—

(a) in the English language text substitute—

“(7) In determining for the purposes of the regulations whether disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this regulation.”,

and

(b) in the Welsh language text substitute—

“(7) Wrth benderfynu at ddibenio paragraff (6) a yw datgeliad wedi’i wahardd, mae i’w dybied at ddibenio paragraff 5(2) o Atodlen 2 i Ddeddf Diogelu Data 2018 a pharagraff 3(2) o Atodlen 11 i’r Ddeddf honno (esemiadau rhag darpariaethau penodol o’r ddeddfwriaeth diogelu data: datgeliadau sy’n ofynnol gan y gyfraith) bod y datgeliad yn ofynnol gan y rheoliad hwn.”

2005 (1) Regulation 29 (occurrence reports) is amended as follows.

(2) In paragraph (3)—

(a) in the English language text, at the end insert “or the GDPR”, and
(b) in the Welsh language text, at the end insert “neu’r GDPR”.

(3) For paragraph (4)—

(a) in the English language text substitute—

“(4) In determining for the purposes of paragraph (3) whether disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this regulation.”,

and

(b) in the Welsh language text substitute—

“(4) Wrth benderfynu at ddibenio paragraff (3) a yw datgeliad wedi’i wahardd, mae i’w dybied at ddibenio paragraff 5(2) o Atodlen 2 i Ddeddf Diogelu Data 2018 a pharagraff 3(2) o Atodlen 11 i’r Ddeddf honno (esemiadau rhag darpariaethau penodol o’r ddeddfwriaeth diogelu data: datgeliadau sy’n ofynnol gan y gyfraith) bod y datgeliad yn ofynnol gan y rheoliad hwn.”

Energy Order 2003 (Supply of Information) Regulations (Northern Ireland) 2008 (S.R. (N.I.) 2008 No. 3) 200T (1) Regulation 5 of the Energy Order 2003 (Supply of Information) Regulations (Northern Ireland) 2008 (information whose disclosure would be affected by the application of other legislation) is amended as follows.

(2) In paragraph (3)—

(a) omit “within the meaning of section 1(1) of the Data Protection Act 1998”, and
(b) for the words from “where” to the end substitute “if the condition in paragraph (3A) or (3B) is satisfied”.

(3) After paragraph (3) insert—

“(3A) The condition in this paragraph is that the disclosure of the information to a member of the public—

(a) would contravene any of the data protection principles, or
(b) would do so if the exemptions in section24(1) of the Data Protection Act 2018 (manual unstructured data held by public authorities) were disregarded.

(3B) The condition in this paragraph is that the disclosure of the information to a member of the public would contravene—

(a) Article 21 of the GDPR (general processing: right to object to processing), or
(b) section99 of the Data Protection Act 2018 (intelligence services processing: right to object to processing).”

(4) After paragraph (4) insert—

“(5) In this regulation—

“the data protection principles” means the principles set out in—

(a) Article 5(1) of the GDPR,
(b) section34(1) of the Data Protection Act 2018, and
(c) section85(1) of that Act;

“the GDPR” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section3(10), (11) and (14) of that Act);

“personal data” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section3(2) and (14) of that Act).”

Companies (Disclosure of Address) Regulations 2009 (S.I. 2009/214) 200U (1) Paragraph 6 of Schedule 2 to the Companies (Disclosure of Address) Regulations 2009 (conditions for permitted disclosure to a credit reference agency) is amended as follows.

(2) The existing text becomes sub-paragraph (1).

(3) In paragraph (b) of that sub-paragraph, for sub-paragraph (ii) substitute—

(i) for the purposes of ensuring that it complies with its data protection obligations;”,

(4) In paragraph (c) of that sub-paragraph—

(a) omit “or” at the end of sub-paragraph (i), and
(b) at the end insert “; or

(i) section145 of the Data Protection Act 2018 (false statements made in response to an information notice);”.

(5) After paragraph (c) of that sub-paragraph insert—

“(d) has not been given a penalty notice under section154 of the Data Protection Act 2018 in circumstances described in paragraph (c)(ii), other than a penalty notice that has been cancelled.”

(6) After sub-paragraph (1) insert—

“(2) In this paragraph, “data protection obligations”, in relation to a credit reference agency, means—

(a) where the agency carries on business in the United Kingdom, obligations under the data protection legislation (as defined in section 3 of the Data Protection Act 2018);

(b) where the agency carries on business in a EEA State other than the United Kingdom, obligations under—

(i) the GDPR (as defined in section3(10) of the Data Protection Act 2018),

(ii) legislation made in exercise of powers conferred on member States under the GDPR (as so defined), and

(iii) legislation implementing the Law Enforcement Directive (as defined in section3(12) of the Data Protection Act 2018).”

Overseas Companies Regulations 2009 (S.I. 2009/1801) 200V (1) Paragraph 6 of Schedule 2 to the Overseas Companies Regulations 2009 (conditions for permitted disclosure to a credit reference agency) is amended as follows.

(2) The existing text becomes sub-paragraph (1).

(3) In paragraph (b) of that sub-paragraph, for sub-paragraph (ii) substitute—

(i) for the purposes of ensuring that it complies with its data protection obligations;”,

(4) In paragraph (c) of that sub-paragraph—

(a) omit “or” at the end of sub-paragraph (i), and
(b) at the end insert “; or

(i) section145 of the Data Protection Act 2018 (false statements made in response to an information notice);”.
(5) After paragraph (c) of that sub-paragraph insert—

“(d) has not been given a penalty notice under section 154 of the Data Protection Act 2018 in circumstances described in paragraph (c)(ii), other than a penalty notice that has been cancelled.”

(6) After sub-paragraph (1) insert—

“(2) In this paragraph, “data protection obligations”, in relation to a credit reference agency, means—

(a) where the agency carries on business in the United Kingdom, obligations under the data protection legislation (as defined in section 3 of the Data Protection Act 2018);

(b) where the agency carries on business in an EEA State other than the United Kingdom, obligations under—

(i) the GDPR (as defined in section 3(10) of the Data Protection Act 2018),

(ii) legislation made in exercise of powers conferred on member States under the GDPR (as so defined), and

(iii) legislation implementing the Law Enforcement Directive (as defined in section 3(12) of the Data Protection Act 2018).”

Provision of Services Regulations 2009 (S.I. 2009/2999)

200W In regulation 25 of the Provision of Services Regulations 2009 (derogations from the freedom to provide services), for paragraph (d) substitute—

“(d) matters covered by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);”

This amendment makes consequential amendments to secondary legislation including to the National Assembly for Wales Commission (Crown Status) Order 2007.

Amendment 223, in schedule 18, page 249, line 32, at end insert—

“INSPIRE (Scotland) Regulations 2009 (S.S.I. 2009/440) 201A (1) Regulation 10 of the INSPIRE (Scotland) Regulations 2009 (public access to spatial data sets and spatial data services) is amended as follows.

(2) In paragraph (2)—

(a) omit “or” at the end of sub-paragraph (a),

(b) for sub-paragraph (b) substitute—

“(b) Article 21 of the GDPR (general processing: right to object to processing), or

(c) section 99 of the Data Protection Act 2018 (intelligence services processing: right to object to processing).”, and

(c) omit the words following sub-paragraph (b).

(3) After paragraph (6) insert—

“(7) In this regulation—

“the data protection principles” means the principles set out in—

(a) Article 5(1) of the GDPR,

(b) section 34(1) of the Data Protection Act 2018, and

(c) section 85(1) of that Act;

“the GDPR” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(10), (11) and (14) of that Act);

“personal data” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2) and (14) of that Act).

(8) In determining for the purposes of this regulation whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article 6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (disappealing the legitimate interests gateway in relation to public authorities) were omitted.”

Controlled Drugs (Supervision of Management and Use) Regulations (Northern Ireland) 2009 (S.R (N.I.) 2009 No. 225)

201B The Controlled Drugs (Supervision of Management and Use) Regulations (Northern Ireland) 2009 are amended as follows.

201C In regulation 2(2) (interpretation), at the appropriate place insert—

“the GDPR” and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(10), (11) and (14) of that Act);”

201D (1) Regulation 25 (duty to co-operate by disclosing information as regards relevant persons) is amended as follows.

(2) In paragraph (7), at the end insert “or the GDPR”.

(3) For paragraph (8) substitute—

“(8) In determining for the purposes of paragraph (7) whether disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this regulation.”

201E (1) Regulation 26 (responsible bodies requesting additional information be disclosed about relevant persons) is amended as follows.

(2) In paragraph (6), at the end insert “or the GDPR”.

(3) For paragraph (7) substitute—

“(7) In determining for the purposes of paragraph (6) whether disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this regulation.”

201F (1) Regulation 29 (occurrence reports) is amended as follows.

(2) In paragraph (3), at the end insert “or the GDPR”.

(3) For paragraph (4) substitute—

“(4) In determining for the purposes of paragraph (3) whether disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this regulation.”

201G The Pharmacy Order 2010 is amended as follows.

201H In article 3(1) (interpretation), omit the definition of “Directive 95/46/EC”.

201I (1) Article 9 (inspection and enforcement) is amended as follows.

(2) For paragraph (4) substitute—

“(4) If a report that the Council proposes to publish pursuant to paragraph (3) includes personal data, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure of the personal data is required by paragraph (3) of this article.”

(3) After paragraph (4) insert—

“(5) In this article, “personal data” and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(2) and (14) of that Act).”

201J In article 33A (European professional card), after paragraph (2) insert—

“(3) In Schedule 2A, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018.”
201K (1) Article 49 (disclosure of information: general) is amended as follows.
(2) In paragraph (2)(a), after “enactment” insert “or the GDPR”.
(3) For paragraph (3) substitute—
“(3) In determining for the purposes of paragraph (2)(a) whether a disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by paragraph (1) of this article.”
(4) After paragraph (5) insert—
“(6) In this article, “the GDPR” and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(10), (11) and (14) of that Act).”
201L (1) Article 55 (professional performance assessments) is amended as follows.
(2) In paragraph (5)(a), after “enactment” insert “or the GDPR”.
(3) For paragraph (6) substitute—
“(6) In determining for the purposes of paragraph (5)(a) whether a disclosure is prohibited, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by paragraph (4) of this article.”
(4) After paragraph (8) insert—
“(9) In this article, “the GDPR” and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(10), (11) and (14) of that Act).”
201M In article 67(6) (Directive 2005/36/EC: designation of competent authority etc.), after sub-paragraph (a) insert—
“(aa) “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018;”.
201N (1) Schedule 2A (Directive 2005/36/EC: European professional card) is amended as follows.
(2) In paragraph 8(1) (access to data), for “Directive 95/46/EC”) substitute “the GDPR”.
(3) In paragraph 9 (processing data)—
(a) omit sub-paragraph (2) (deeming the Council to be the controller for the purposes of Directive 95/46/EC), and
(b) after sub-paragraph (2) insert—
“(3) In this paragraph, “personal data” has the same meaning as in the Data Protection Act 2018 (see section 3(2) of that Act).”
201O (1) The table in Schedule 3 (Directive 2005/36/EC: designation of competent authority etc.) is amended as follows.
(2) In the entry for Article 56(2), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.
(3) In the entry for Article 56a(4), in the second column, for “Directive 95/46/EC” substitute “the GDPR”.
National Employment Savings Trust Order 2010 (S.I. 2010/917)
201P The National Employment Savings Trust Order 2010 is amended as follows.
201Q In article 2 (interpretation)—
(a) omit the definition of “data” and “personal data”, and
(b) at the appropriate place insert—
“personal data” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2) and (14) of that Act).”
201R (1) Article 10 (disclosure of requested data to the Secretary of State) is amended as follows.
(2) In paragraph (1)—
(a) for “disclosure of data” substitute “disclosure of information”, and
(b) for “requested data” substitute “requested information”.
(3) In paragraph (2)—
(a) for “requested data” substitute “requested information”,
(b) for “those data are” substitute “the information is”, and
(c) for “receive those data” substitute “receive that information”.
(4) In paragraph (3), for “requested data” substitute “requested information”.
(5) In paragraph (4), for “requested data” substitute “requested information”.
Local Elections (Northern Ireland) Order 2010 (S.I. 2010/2977)
201S (1) Schedule 3 to the Local Elections (Northern Ireland) Order 2010 (access to marked registers and other documents open to public inspection after an election) is amended as follows.
(2) In paragraph 1(1) (interpretation and general)—
(a) omit the definition of “research purposes”, and
(b) at the appropriate places insert—
“Article 89 GDPR purposes” means the purposes mentioned in Article 59(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”;
“the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);”.
(3) In paragraph 5(3) (restrictions on the use, supply and disclosure of documents open to public inspection, for “research purposes” substitute “Article 89 GDPR purposes”.
Pupil Information (Wales) Regulations 2011 (S.I. 2011/1942 (W.209))
201T (1) Regulation 5 of the Pupil Information (Wales) Regulations 2011 (duties of head teacher - educational records) is amended as follows.
(2) In paragraph (5)—
(a) in the English language text, for “documents which are subject to any order under section 30(2) of the Data Protection Act 1998” substitute “information—
(b) which the head teacher could not lawfully disclose to the pupil under the GDPR, or
(b) to which the pupil would have no right of access under the GDPR,”.
(b) in the Welsh language text, for “ddogfennau sy’n dderbynogi ei unrhyw ochrwmyn o dan adran 30(2) o Ddeddf Ddogelau Data 1998” substitute “wybodaeth—
(a) na allai’r pennaeth ei datgelu’n gyfreithlon i’r disgybl o dan y GDPR, neu
(b) na fyddai gan y disgybl hawl mynediad ati o dan y GDPR.”
(3) After paragraph (5)—
(a) in the English language text insert—
“(6) In this regulation, “the GDPR” (“y GDPR”) means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018;”.
(b) in the Welsh language text insert—
“(6) Yn y rheoliad hwn, ystyri gy y GDPR (“the GDPR”) yw Rheoliad (EU) 2016/679 Senedd Ewrop a’r Cyngor dyddiedig 27 Ebrill 2016 ar ddigolgu personau naturiol o ran prosesu data personol a rhuddid symud data o’r fath (y Rheoliad Diogelu Data Cyflydredinol), fel y’i darllenir ynglŷd à Phennoedd 2 o Ran 2 o Ddeffed Diogelu Data 2018.”

Debt Arrangement Scheme (Scotland) Regulations 2011 (S.S.I. 2011/141)

201U In Schedule 4 to the Debt Arrangement Scheme (Scotland) Regulations 2011 (payments distributors), omit paragraph 2.

Police and Crime Commissioner Elections Order 2012 (S.I. 2012/1917)

201V The Police and Crime Commissioner Elections Order 2012 is amended as follows.

201W (1) Schedule 2 (absent voting in Police and Crime Commissioner elections) is amended as follows.

(2) In paragraph 20 (absent voter lists: supply of copies etc)—

(a) in sub-paragraph (8), for paragraph (a) (but not the final “or”) substitute—

(a) purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics); , and

(b) after sub-paragraph (10) insert—

“(11) In this paragraph, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).”

(3) In paragraph 24 (restriction on use of absent voter records or lists or the information contained in them)—

(a) in sub-paragraph (3), for paragraph (a) (but not the final “or”) substitute—

(a) purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics); , and

(b) after that sub-paragraph insert—

“(4) In this paragraph, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data (General Data Protection Regulation).”

(3) In paragraph 24 (restriction on use of absent voter records or lists or the information contained in them)—

(a) in sub-paragraph (3), for paragraph (a) (but not the final “or”) substitute—

(a) purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics); , and

(b) after that sub-paragraph insert—

“(5) In this paragraph, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data (General Data Protection Regulation).”

Neighbourhood Planning (Referendums) Regulations 2012 (S.I. 2012/2031)

201Y Schedule 6 to the Neighbourhood Planning (Referendums) Regulations 2012 (registering to vote in a business referendum) is amended as follows.

2012 (1) Paragraph 29(1) (interpretation of Part 8) is amended as follows.

(2) At the appropriate places insert—

“‘Article 89 GDPR purposes’ means the purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);” .

“‘the GDPR’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data (General Data Protection Regulation);”.

(3) For the definition of “relevant conditions” substitute—

“‘relevant requirement’ means the requirement under Article 89 of the GDPR, read with section 19 of the Data Protection Act 2018, that personal data processed for Article 89 GDPR purposes must be subject to appropriate safeguards;.”

(4) Omit the definition of “research purposes”.

201AA In paragraph 32(3)(b)(i), for “section 11(3) of the Data Protection Act 1998” substitute “section 123(5) of the Data Protection Act 2018”.

201AB In paragraph 34(6) and (7) (supply of copy of business voting register to public libraries and local authority archives services and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 201AC In paragraph 34(6) and (7) (supply of copy of business voting register to the Office of National Statistics and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 201AD In paragraph 39(8) and (9) (supply of copy of business voting register to public libraries and local authority archives services and restrictions on use), for “research purposes in compliance with the relevant conditions” substitute “Article 89 GDPR purposes in accordance with the relevant requirement”. 201AE In paragraph 45(2) (conditions on the use, supply and disclosure of documents open to public inspection), for paragraph (a) (but not the final “or”) substitute—

(a) Article 89 GDPR purposes (as defined in paragraph 29).”.

Controlled Drugs (Supervision of Management and Use) Regulations 2013 (S.I. 2013/373)

201AF (1) Regulation 20 of the Controlled Drugs (Supervision of Management and Use) Regulations 2013 (information management) is amended as follows.

(2) For paragraph (4) substitute—

“(4) Where a CDAO, a responsible body or someone acting on their behalf is permitted to share information which includes personal data by virtue of a function under these Regulations, it is to be assumed for the purposes of paragraph 5(2) of Schedule 2 to the Data Protection Act 2018 and paragraph 3(2) of Schedule 11 to that Act (exemptions from certain provisions of the data protection legislation: disclosures required by law) that the disclosure is required by this regulation.”

(3) In paragraph (5), after “enactment” insert “or the GDPR”.

(4) After paragraph (6) insert—

“(7) In this regulation, “the GDPR”, “personal data” and references to Schedule 2 to the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(2), (10), (11) and (14) of that Act).”


201AG (1) Article 3 of the Communications Act 2003 (Disclosure of Information) Order 2014 (specification of relevant functions) is amended as follows.

(2) The existing text becomes paragraph (1).

(3) In that paragraph, in sub-paragraph (a), for “the Data Protection Act 1998” substitute “the data protection legislation”.

(4) After that paragraph insert—

“(2) In this article, “the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act).”

This amendment makes consequential amendments to secondary legislation.
Amendment 224, in schedule 18, page 250, line 7, at end insert—

"Companies (Disclosure of Date of Birth Information) Regulations 2015 (S.I. 2015/1694)

204A (1) Paragraph 6 of Schedule 2 to the Companies (Disclosure of Date of Birth Information) Regulations 2015 (conditions for permitted disclosure to a credit reference agency) is amended as follows.

(2) The existing text becomes sub-paragraph (1).

(3) In paragraph (b) of that sub-paragraph, for sub-paragraph (ii) substitute—

(i) for the purposes of ensuring that it complies with its data protection obligations;”;

(4) In paragraph (c) of that sub-paragraph—

(a) omit “or” at the end of sub-paragraph (i), and

(b) at the end insert “; or

(i) section 145 of the Data Protection Act 2018 (false statements made in response to an information notice);”;

(5) After paragraph (c) of that sub-paragraph insert—

“(d) has not been given a penalty notice under section 154 of the Data Protection Act 2018 in circumstances described in paragraph (c)(ii), other than a penalty notice that has been cancelled.”

(6) After sub-paragraph (1) insert—

“(2) In this paragraph, “data protection obligations”, in relation to a credit reference agency, means—

(a) where the agency carries on business in the United Kingdom, obligations under the data protection legislation (as defined in section 3 of the Data Protection Act 2018);

(b) where the agency carries on business in a EEA State other than the United Kingdom, obligations under—

(i) the GDPR (as defined in section 3(10) of the Data Protection Act 2018),

(ii) legislation made in exercise of powers conferred on member States under the GDPR (as so defined), and

(iii) legislation implementing the Law Enforcement Directive (as defined in section 3(12) of the Data Protection Act 2018).”

Small and Medium Sized Business (Credit Information) Regulations 2015 (S.I. 2015/1945)

204B The Small and Medium Sized Business (Credit Information) Regulations 2015 are amended as follows.

(1) Schedule 12 (criteria for the designation of a credit reference agency) is amended as follows.

(2) In paragraph (1)(b), for “the Data Protection Act 1998” substitute “the data protection legislation”.

(3) After paragraph (2) insert—

“(3) In this regulation, “the data protection legislation” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act).”

204D (1) Regulation 15 (access to and correction of information for individuals and small firms) is amended as follows.

(2) For paragraph (1) substitute—

“(1) Section 13 of the Data Protection Act 2018 (rights of the data subject under the GDPR: obligations of credit reference agencies) applies in respect of a designated credit reference agency which is not a credit reference agency within the meaning of section 145(8) of the Consumer Credit Act 1974 as if it were such an agency.”

(3) After paragraph (3) insert—

“(4) In this regulation, the reference to section 13 of the Data Protection Act 2018 has the same meaning as in Parts 5 to 7 of that Act (see section 3(14) of that Act).”

European Union (Recognition of Professional Qualifications) Regulations 2015 (S.I. 2015/2059)

204E The European Union (Recognition of Professional Qualifications) Regulations 2015 are amended as follows.

204F (1) Regulation 2(1) (interpretation) is amended as follows.

(2) Omit the definition of “Directive 95/46/EC”.

(3) At the appropriate place insert—

“the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), read with Chapter 2 of Part 2 of the Data Protection Act 2018.”

204G In regulation 5(5) (functions of competent authorities in the United Kingdom) for “Directives 95/46/EC” substitute “the GDPR and Directive”.

204H In regulation 45(3) (processing and access to data regarding the European Professional Card), for “Directive 95/46/EC” substitute “the GDPR”.

204I In regulation 46(1) (processing and access to data regarding the European Professional Card), for “Directive 95/46/EC” substitute “the GDPR”.

204J In regulation 48(2) (processing and access to data regarding the European Professional Card), omit paragraph (2) (deeming the relevant designated competent authorities to be controllers for the purposes of Directive 95/46/EC).

204K In regulation 66(3) (exchange of information), for “Directives 95/46/EC” substitute “the GDPR and Directive”. Scottish Parliament (Elections etc) Order 2015 (S.S.I. 2015/425)

204L The Scottish Parliament (Elections etc) Order 2015 is amended as follows.

204M (1) Schedule 3 (absent voting) is amended as follows.

(2) In paragraph 16 (absent voting lists: supply of copies etc)—

(a) in sub-paragraph (4), for paragraph (a) (but not the final “or”) substitute—

(a) purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”;

(b) after sub-paragraph (10) insert—

“(11) In this paragraph, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).”

(3) In paragraph 20 (restriction on use of absent voting lists)—

(a) in sub-paragraph (3), for paragraph (a) (but not the final “or”) substitute—

(a) purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”;

(b) after that sub-paragraph insert—

“(4) In this paragraph, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).”

204N (1) Schedule 8 (access to marked registers and other documents open to public inspection after an election) is amended as follows.

(2) In paragraph 1(2) (interpretation), omit paragraphs (c) and (d) (but not the final “and”).

(3) In paragraph 5 (restriction on use of documents or of information contained in them)—

(a) in sub-paragraph (3), for paragraph (a) (but not the final “or”) substitute—

(a) purposes mentioned in Article 89(1) of the GDPR (archiving in the public interest, scientific or historical research and statistics);”;

(b) after the sub-paragraph insert—

“(4) In this paragraph, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the processing of personal data and on the free movement of such data (General Data Protection Regulation).”

204P (1) Schedule 18, page 250, line 7, at end insert—

“(archiving in the public interest, scientific or historical research and statistics);”, and
(b) after sub-paragraph (4) insert—
“(5) In this paragraph, “the GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).”

Recall of MPs Act 2015 (Recall Petition) Regulations 2016 (S.I. 2016/295)

204O In paragraph 1(3) of Schedule 3 to the Recall of MPs Act 2015 (Recall Petition) Regulations 2016 (access to marked registers after a petition), omit the definition of “relevant conditions”.

Register of People with Significant Control Regulations 2016 (S.I. 2016/339)

204P Schedule 4 to the Register of People with Significant Control Regulations 2016 (conditions for permitted disclosure) is amended as follows.

204Q (1) Paragraph 6 (disclosure to a credit reference agency) is amended as follows.

(2) In sub-paragraph (b), for paragraph (ii) (together with the final “;” and “)”) substitute—
(i) for the purposes of ensuring that it complies with its data protection obligations;“;

(3) In sub-paragraph (c) (a) “or” at the end of paragraph (ii), and

(b) at the end insert “; or

(i) section 145 of the Data Protection Act 2018 (false statements made in response to an information notice); and”.

(4) After sub-paragraph (c) insert—
“(d) has not been given a penalty notice under section 154 of the Data Protection Act 2018 in circumstances described in sub-paragraph (c)(iii), other than a penalty notice that has been cancelled.”

Recall of MPs Act 2015 (Recall Petition) Regulations 2016 (S.I. 2016/295)

204R In paragraph 12A (disclosure to a credit reference agency or a financial institution, for sub-paragraph (b) substitute—
(b) for the purposes of ensuring that it complies with its data protection obligations.”

204S (1) In Part 3 (interpretation), after paragraph 13 insert—
14 In this Schedule, “data protection obligations”, in relation to a credit reference agency, a credit institution or a financial institution, means—

(a) where the agency or institution carries on business in the United Kingdom, obligations under the data protection legislation (as defined in section 3 of the Data Protection Act 2018);

(b) where the agency or institution carries on business in an EEA State other than the United Kingdom, obligations under—
(i) the GDPR (as defined in section 3(10) of the Data Protection Act 2018),

(ii) legislation made in exercise of powers conferred on member States under the GDPR (as so defined), and

(iii) legislation implementing the Law Enforcement Directive (as defined in section 3(12) of the Data Protection Act 2018).”

Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (S.I. 2016/696)

204T The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 are amended as follows.

204U In regulation 2(1) (interpretation), omit the definition of “the 1998 Act”.

204V In regulation 3(3) (supervision), omit “under the 1998 Act”.

204W For Schedule 2 substitute—

SCHEDULE 2

INFORMATION COMMISSIONER’S ENFORCEMENT POWERS

Provisions applied for enforcement purposes

1 For the purposes of enforcing these Regulations and the eIDAS Regulation, the following provisions of Parts 5 to 7 of the Data Protection Act 2018 apply with the modifications set out in paragraphs 2 to 24—

(a) section 140 (publication by the Commissioner);

(b) section 141 (notices from the Commissioner);

(c) section 143 (information notices);

(d) section 144 (information notices: restrictions);

(e) section 145 (false statements made in response to an information notice);

(f) section 146 (assessment notices);

(g) section 147 (assessment notices: restrictions);

(h) section 148 (enforcement notices);

(i) section 149 (enforcement notices: supplementary);

(j) section 151 (enforcement notices: restrictions);

(k) section 152 (enforcement notices: cancellation and variation);

(l) section 153 and Schedule 15 (powers of entry and inspection);

(m) section 154 and Schedule 16 (penalty notices);

(n) section 155(4)(a) (penalty notices: restrictions);

(o) section 156 (maximum amount of penalty);

(p) section 158 (amount of penalties: supplementary);

(q) section 159 (guidance about regulatory action);

(r) section 160 (approval of first guidance about regulatory action);

(s) section 161 (rights of appeal);

(t) section 162 (determination of appeals);

(u) section 179(1), (2), (5), (7) and (12) (regulations and consultation);

(v) section 189 (penalties for offences);

(w) section 190 (prosecution);

(x) section 195 (proceedings in the First-tier Tribunal: contempt);

(y) section 196 (Tribunal Procedure Rules).

General modification of references to the Data Protection Act 2018

2 The provisions listed in paragraph 1 have effect as if—

(a) references to the Data Protection Act 2018 were references to the provisions of that Act as applied by these Regulations;

(b) references to a particular provision of that Act were references to that provision as applied by these Regulations.

Modification of section 143 (information notices)

3 (1) Section 143 has effect as if subsections (9) and (10) were omitted.

(2) In that section, subsection (1) has effect as if—

(a) in paragraph (a)—

(i) for “controller or processor” there were substituted “trust service provider”; and

(ii) for “the data protection legislation” there were substituted “the eIDAS Regulation and the EITSET Regulations”;

(b) paragraph (b) were omitted.

Modification of section 144 (information notices: restrictions)

4 (1) Section 144 has effect as if subsections (1) and (9) were omitted.

(2) In that section—

(a) subsections (3)(b) and (4)(b) have effect as if for “the data protection legislation” there were substituted “the eIDAS Regulation or the EITSET Regulations”;

(b) subsection (7)(a) has effect as if for “this Act” there were substituted “section 145 or paragraph 15 of Schedule 15”;

(c) subsection (8) has effect as if for “this Act (other than an offence under section 145)” there were substituted “paragraph 15 of Schedule 15”.

SCHEDULE 2
Modification of section 146 (assessment notices)
5 (1) Section 146 has effect as if subsection (10) were omitted.
(2) In that section—
(a) subsection (1) has effect as if—
(i) for “controller or processor” (in both places) there were substituted “trust service provider”;
(ii) for “the data protection legislation” there were substituted “the eIDAS requirements”;
(b) subsection (2) has effect as if paragraphs (g) and (h) were omitted;
(c) subsections (7), (8) and (9) have effect as if for “controller or processor” (in each place) there were substituted “trust service provider”.

Modification of section 147 (assessment notices: restrictions)
6 (1) Section 147 has effect as if subsections (5) and (6) were omitted.
(2) In that section, subsections (2)(b) and (3)(b) have effect as if for “the data protection legislation” there were substituted “the eIDAS Regulation or the EITSET Regulations”.

Modification of section 148 (enforcement notices)
7 (1) Section 148 has effect as if subsections (2) to (5) and (7) to (9) were omitted.
(2) In that section—
(a) subsection (1) has effect as if—
(i) for “as described in subsection (2), (3), (4) or (5)” there were substituted “to comply with the eIDAS requirements”;
(ii) for “sections 149 and 150” there were substituted “section 149”;
(b) subsection (6) has effect as if the words “given in reliance on subsection (2), (3) or (5)” were omitted.

Modification of section 149 (enforcement notices: supplementary)
8 (1) Section 149 has effect as if subsection (3) were omitted.
(2) In that section, subsection (2) has effect as if the words “in reliance on section 148(2)” and “or distress” were omitted.

Modification of section 151 (enforcement notices: restrictions)
9 Section 151 has effect as if subsections (1), (2) and (4) were omitted.

Withdrawal notices
10 The provisions listed in paragraph 1 have effect as if after section 152 there were inserted—

“Withdrawal notices
152A Withdrawal notices
(1) The Commissioner may, by written notice (a “withdrawal notice”), withdraw the qualified status from a trust service provider, or the qualified status of a service provider provided by a trust service provider, if—
(a) the Commissioner is satisfied that the trust service provider has failed to comply with an information notice or an enforcement notice, and
(b) the condition in subsection (2) or (3) is met.
(2) The condition in this subsection is met if the period for the trust service provider to appeal against the information notice or enforcement notice has ended without an appeal having been brought.
(3) The condition in this subsection is met if an appeal against the information notice or enforcement notice has been brought and—
(a) the appeal and any further appeal in relation to the notice has been decided or has otherwise ended, and
(b) the time for appealing against the result of the appeal or further appeal has ended without another appeal having been brought.
(4) A withdrawal notice must—
(a) state when the withdrawal takes effect, and
(b) provide information about the rights of appeal under section 161.”

Modification of Schedule 15 (powers of entry and inspection)
11 (1) Schedule 15 has effect as if paragraph 3 were omitted.
(2) Paragraph 1(1) of that Schedule (issue of warrants in connection with non-compliance and offences) has effect as if for paragraph (a) (but not the final “and”) there were substituted—
(a) there are reasonable grounds for suspecting that—
(i) a trust service provider has failed or is failing to comply with the eIDAS requirements, or
(ii) an offence under section 145 or paragraph 15 of Schedule 15 has been or is being committed,.
(3) Paragraph 2 of that Schedule (issue of warrants in connection with assessment notices) has effect as if—
(a) in sub-paragraph (1) and (2), for “controller or processor” there were substituted “trust service provider”;
(b) in sub-paragraph (2), for “the data protection legislation” there were substituted “the eIDAS requirements”.
(4) Paragraph 5 of that Schedule (content of warrants) has effect as if—
(a) in sub-paragraph (1)(c), for “the processing of personal data” there were substituted “the provision of trust services”;
(b) in sub-paragraph (2)(c)—
(i) for “controller or processor” there were substituted “trust service provider”;
(ii) for “as described in section 148(2)” there were substituted “to comply with the eIDAS requirements”;
(c) in sub-paragraph (3)(a) and (c)—
(i) for “controller or processor” there were substituted “trust service provider”;
(ii) for “the data protection legislation” there were substituted “the eIDAS requirements”.
(5) Paragraph 11 of that Schedule (privileged communications) has effect as if, in sub-paragraphs (1)(b) and (2)(b), for “the data protection legislation” there were substituted “the eIDAS Regulation or the EITSET Regulations”.

Modification of section 154 (penalty notices)
12 (1) Section 154 has effect as if subsections (1)(a), (2)(a), (3)(g), (3A) and (5) to (7) were omitted.
(2) Subsection (2) of that section has effect as if—
(a) the words “Subject to subsection (3A),” were omitted;
(b) in paragraph (b), the words “to the extent that the notice concerns another matter,” were omitted.
(3) Subsection (3) of that section has effect as if—
(a) for “controller or processor”, in each place, there were substituted “trust service provider”; 
(b) in paragraph (c), the words “or distress” were omitted;
(c) in paragraph (c), for “data subjects” there were substituted “relying parties”;
(d) in paragraph (d), for “section 57, 66, 103 or 107” there were substituted “Article 19(1) of the eIDAS Regulation”.

Modification of Schedule 16 (penalties)
13 Schedule 16 has effect as if paragraphs 3(2)(b) and 5(2)(b) were omitted.

Modification of section 156 (maximum amount of penalty)
14 Section 156 has effect as if subsections (1) to (3) and (6) were omitted.

Modification of section 158 (amount of penalties: supplementary)
15 Section 158 has effect as if—
(a) in subsection (1), the words “Article 83 of the GDPR” and “were omitted;
(b) in subsection (2), the words “Article 83 of the GDPR” and “and section 157” were omitted.

Modification of section 159 (guidance about regulatory action)
16 (1) Section 159 has effect as if subsections (4) and (10) were omitted.
(2) In that section, subsection (3)(e) has effect as if for “controllers and processors” there were substituted “trust service providers”.

Modification of section161 (rights of appeal)

17 (1) Section 161 has effect as if subsection (5) were omitted.

(2) In that section, subsection (1) has effect as if, after paragraph (c), there were inserted—

(a) a withdrawal notice;“.

Modification of section162 (determination of appeals)

18 Section162 has effect as if subsection (7) were omitted.

Modification of section179 (regulations and consultation)

19 Section179 has effect as if subsections (3), (4), (6), (8) to (11) and (13) were omitted.

Modification of section189 (penalties for offences)

20 (1) Section 189 has effect as if subsections (3) to (5) were omitted.

(2) In that section—

(a) subsection (1) has effect as if the words “section 119 or 173” were omitted;

(b) subsection (2) has effect as if for “section 132, 145, 170, 171 or 181” there were substituted “section 145”.

Modification of section190 (prosecution)

21 Section190 has effect as if subsections (3) to (6) were omitted.

Modification of section195 (proceedings in the First-tier Tribunal: contempt)

22 Section195 has effect as if in subsection (1)(a), for sub-paragraphs (i) and (ii) there were substituted “on an appeal under section161”.

Modification of section196 ( Tribunal Procedure Rules)

23 Section196 has effect as if—

(a) in subsection (1), for paragraphs (a) and (b) there were substituted “the exercise of the rights of appeal conferred by section 161”;

(b) in subsection (2)(a) and (b), for “the processing of personal data” there were substituted “the provision of trust services”.

Approval of first guidance about regulatory action

24 (1) This paragraph applies if the first guidance produced under section 159(1) of the Data Protection Act 2018 and the first guidance produced under that provision as applied by this Schedule are laid before Parliament as a single document (“the combined guidance”).

(2) Section 160 of that Act (including that section as applied by this Schedule) has effect as if the references to “the guidance” were references to the combined guidance, except in subsections (2)(b) and (4).

(3) Nothing in subsection (2)(a) of that section (including as applied by this Schedule) prevents another version of the combined guidance being laid before Parliament.

(4) Any duty under subsection (2)(b) of that section (including as applied by this Schedule) may be satisfied by producing another version of the combined guidance.

Interpretation

25 In this Schedule—

“the eIDAS requirements” means the requirements of Chapter III of the eIDAS Regulation;

“the EITFIT Regulations” means these Regulations;

“withdrawal notice” has the meaning given in section 146A of the Data Protection Act 2018 (as inserted in that Act by this Schedule).”

Court Files Privileged Access Rules (Northern Ireland) 2016 (S.R. (N.I.) 2016 No. 121)

204X The Court Files Privileged Access Rules (Northern Ireland) 2016 are amended as follows.

204Y In rule 5 (information that may released) for “Schedule 1 of the Data Protection Act 1998” substitute “—

(a) Article 5(1) of the GDPR, and

(b) section34(1) of the Data Protection Act 2018.”

204Z In rule 7(2) (provision of information) for “Schedule 1 of the Data Protection Act 1998” substitute “—

(a) Article 5(1) of the GDPR, and

(b) section34(1) of the Data Protection Act 2018.”

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (S.I. 2017/692)

204AA The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 are amended as follows.

204AB In regulation 3(1) (interpretation), at the appropriate places insert—

“(6) Before establishing a business relationship or entering into an occasional transaction with a new customer, as well as providing the customer with the information required under Article 13 of the GDPR (information to be provided where personal data are collected from the data subject), relevant persons must provide the customer with a statement that any personal data received from the customer will be processed only—

(a) for the purposes of preventing money laundering or terrorist financing, or

(b) as permitted under paragraph (3).

(7) In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest includes processing of personal data in accordance with these Regulations that is necessary for the prevention of money laundering or terrorist financing.

(8) In the case of sensitive processing of personal data for the purposes of the prevention of money laundering or terrorist financing, section 10 of, and Schedule 1 to, the Data Protection Act 2018 make provision about when the processing meets a requirement in Article 9(2) or 10 of the GDPR for authorisation under the law of the United Kingdom (see, for example, paragraphs 9, 10 and 10A of that Schedule).”

In this regulation—

“data subject” has the same meaning as in the Data Protection Act 2018 (see section3 of that Act);
“personal data” and “processing” have the same meaning as in Parts 5 to 7 of that Act (see section 3(2), (4) and (14) of that Act); “sensitive processing” means the processing of personal data described in Article 9(1) or 10 of the GDPR (special categories of personal data relating to criminal convictions and offences etc.).

204AL The National Health Service (General Medical Services Contracts) (Scotland) Regulations 2018 (S.S.I. 2018/66)

204AM (1) Regulation 1 (citation and commencement) is amended as follows.

(2) In paragraph (2), omit “Subject to paragraph (3),”.

(3) Omit paragraph (3).

204AN In regulation 3(1) (interpretation)—

(a) omit the definition of “the 1998 Act”,

(b) at the appropriate place insert—

“‘the data protection legislation’ has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);”, and

(c) omit the definition of “GDPR”.

204AO (1) Schedule 6 (other contractual terms) is amended as follows.

(2) In paragraph 63(2) (interpretation; general), for “the 1998 Act or any directly applicable EU instrument relating to data protection” substitute “—

(a) the data protection legislation, or

(b) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection.”

(3) For paragraph 64 (meaning of data controller etc.) substitute—

“Meaning of controller etc.

64A For the purposes of this Part—

“controller” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(6) and (14) of that Act); “data protection officer” means a person designated as a data protection officer under the data protection legislation; “personal data” and “processing” have the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2), (4) and (14) of that Act).”

(4) In paragraph 65(2)(b) (roles, responsibilities and obligations; general), for “data controllers” substitute “controllers”.

(5) In paragraph 69(2)(a) (processing and access of data), for “the 1998 Act, and any directly applicable EU instrument relating to data protection” substitute “—

(i) the data protection legislation, and

(ii) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection;”.

(6) In paragraph 94(4) (variation of a contract: general)—

(a) omit paragraph (b), and

(b) after paragraph (d) (but before the final “and”) insert—

“(da) the data protection legislation;

(db) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection;”.

National Health Service (General Medical Services Contracts) (Scotland) Regulations 2018 (S.S.I. 2018/67)

204AP The National Health Service (Primary Medical Services Section 17C Agreements) (Scotland) Regulations 2018 (S.S.I. 2018/67).

204AO (1) Schedule 6 (other contractual terms) is amended as follows.

(2) In paragraph 63(2) (interpretation; general), for “the 1998 Act or any directly applicable EU instrument relating to data protection” substitute “—

(a) the data protection legislation, or

(b) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection.”

(3) For paragraph 64 (meaning of data controller etc.) substitute—

“Meaning of controller etc.

64A For the purposes of this Part—

“controller” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(6) and (14) of that Act); “data protection officer” means a person designated as a data protection officer under the data protection legislation; “personal data” and “processing” have the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2), (4) and (14) of that Act).”

(4) In paragraph 65(2)(b) (roles, responsibilities and obligations; general), for “data controllers” substitute “controllers”.

(5) In paragraph 69(2)(a) (processing and access of data), for “the 1998 Act, and any directly applicable EU instrument relating to data protection” substitute “—

(i) the data protection legislation, and

(ii) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection;”.

(6) In paragraph 94(4) (variation of a contract: general)—

(a) omit paragraph (b), and

(b) after paragraph (d) (but before the final “and”) insert—

“(da) the data protection legislation;

(db) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection;”.

National Health Service (Primary Medical Services Section 17C Agreements) (Scotland) Regulations 2018 (S.S.I. 2018/67).

204AO (1) Schedule 6 (other contractual terms) is amended as follows.

(2) In paragraph 63(2) (interpretation; general), for “the 1998 Act or any directly applicable EU instrument relating to data protection” substitute “—

(a) the data protection legislation, or

(b) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection.”

(3) For paragraph 64 (meaning of data controller etc.) substitute—

“Meaning of controller etc.

64A For the purposes of this Part—

“controller” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(6) and (14) of that Act); “data protection officer” means a person designated as a data protection officer under the data protection legislation; “personal data” and “processing” have the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2), (4) and (14) of that Act).”

(4) In paragraph 65(2)(b) (roles, responsibilities and obligations; general), for “data controllers” substitute “controllers”.

(5) In paragraph 69(2)(a) (processing and access of data), for “the 1998 Act, and any directly applicable EU instrument relating to data protection” substitute “—

(i) the data protection legislation, and

(ii) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection;”.

(6) In paragraph 94(4) (variation of a contract: general)—

(a) omit paragraph (b), and

(b) after paragraph (d) (but before the final “and”) insert—

“(da) the data protection legislation;

(db) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection;”.

National Health Service (Primary Medical Services Section 17C Agreements) (Scotland) Regulations 2018 (S.S.I. 2018/67).

204AO (1) Schedule 6 (other contractual terms) is amended as follows.

(2) In paragraph 63(2) (interpretation; general), for “the 1998 Act or any directly applicable EU instrument relating to data protection” substitute “—

(a) the data protection legislation, or

(b) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection.”

(3) For paragraph 64 (meaning of data controller etc.) substitute—

“Meaning of controller etc.

64A For the purposes of this Part—

“controller” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(6) and (14) of that Act); “data protection officer” means a person designated as a data protection officer under the data protection legislation; “personal data” and “processing” have the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2), (4) and (14) of that Act).”

(4) In paragraph 65(2)(b) (roles, responsibilities and obligations; general), for “data controllers” substitute “controllers”.

(5) In paragraph 69(2)(a) (processing and access of data), for “the 1998 Act, and any directly applicable EU instrument relating to data protection” substitute “—

(i) the data protection legislation, and

(ii) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection;”.

(6) In paragraph 94(4) (variation of a contract: general)—

(a) omit paragraph (b), and

(b) after paragraph (d) (but before the final “and”) insert—

“(da) the data protection legislation;

(db) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection;”.

National Health Service (Primary Medical Services Section 17C Agreements) (Scotland) Regulations 2018 (S.S.I. 2018/67).
(ii) before paragraph (a) insert—
(iii) for paragraph (d) substitute—
(b) omit sub-paragraphs (2) and (3),
(c) in sub-paragraph (4), for “the 1998 Act and any directly applicable EU instrument relating to data protection” substitute “—
(a) the data protection legislation, or
(b) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection.”,
(d) in sub-paragraph (6)(b), for “data controllers” substitute “controllers”.
(3) In paragraph 37(2)(a) (processing and access of data), for “the 1998 Act, and any directly applicable EU instrument relating to data protection;” substitute “—
(i) the data protection legislation, and
(ii) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection.”.
(4) In paragraph 61(3) (variation of agreement: general)—
(a) omit paragraph (b), and
(b) after paragraph (d) (but before the final “and”) insert—
“(da) the data protection legislation;
(db) any directly applicable EU legislation which is not part of the data protection legislation but which relates to data protection.”.

PART 3
MODIFICATIONS

Introduction

204A(T) (1) Unless the context otherwise requires, legislation described in sub-paragraph (2) has effect on and after the day on which this Part of this Schedule comes into force as if it were modified in accordance with this Part of this Schedule.

(2) That legislation is—
(a) subordinate legislation made before the day on which this Part of this Schedule comes into force;
(b) primary legislation that is passed or made before the end of the Session in which this Act is passed.

(3) In this Part of this Schedule—
“primary legislation” has the meaning given in section 204(7);
“references” includes any references, however expressed.

General modifications

204A(U) (1) References to a particular provision of, or made under, the Data Protection Act 1998 have effect as references to the equivalent provision or provisions of, or made under, the data protection legislation.

(2) Other references to the Data Protection Act 1998 have effect as references to the data protection legislation.

(3) References to disclosure, use or other processing of information that is prohibited or restricted by an enactment which include disclosure, use or other processing of information that is prohibited or restricted by the Data Protection Act 1998 have effect as if they included disclosure, use or other processing of information that is prohibited or restricted by the GDPR or the applied GDPR.

Specific modifications of references to terms used in the Data Protection Act 1998

204A(V) (1) References to personal data, and to the processing of such data, as defined in the Data Protection Act 1998, have effect as references to personal data, and to the processing of such data, as defined for the purposes of Parts 5 to 7 of this Act (see section 3(6) and (14)),

(2) References to processing as defined in the Data Protection Act 1998, in relation to information, have effect as references to processing as defined in section 3(4),

(3) References to a data subject as defined in the Data Protection Act 1998 have effect as references to a data subject as defined in section 3(5),

(4) References to a data controller as defined in the Data Protection Act 1998 have effect as references to a controller as defined for the purposes of Parts 5 to 7 of this Act (see section 3(6) and (14)),

(5) References to the data protection principles set out in the Data Protection Act 1998 have effect as references to the principles set out in—
(a) Article 5(1) of the GDPR and the applied GDPR, and
(b) sections 34(1) and 85(1) of this Act.

(6) References to direct marketing as defined in section 11 of the Data Protection Act 1998 have effect as references to direct marketing as defined in section 123 of this Act.

(7) References to a health professional within the meaning of section 69(1) of the Data Protection Act 1998 have effect as references to a health professional within the meaning of section 197 of this Act.

(8) References to a health record within the meaning of section 68(2) of the Data Protection Act 1998 have effect as references to a health record within the meaning of section 198 of this Act.
'(2A) Sections (Representation of data subjects with their authority: collective proceedings) and (Duty to review provision for representation of data subjects) extend to England and Wales and Northern Ireland only.”

This amendment and Amendment 73 provide that NC1 and NC2 extend only to England and Wales and Northern Ireland.

Amendment 227, in clause 207, page 121, line 15, after “extent” insert “in the United Kingdom”

This amendment and amendments 226, 228 and 229 clarify that amendments of enactments made by the bill have the same extent in the United Kingdom as the enactment amended and that certain amendments also extend to the Isle of Man.

Amendment 228, in clause 207, page 121, line 16, leave out “(ignoring extent by virtue of an Order in Council)”

See the explanatory statement for amendment 227.

Amendment 229, in clause 207, page 121, line 17, at end insert—

'(3A) This subsection and the following provisions also extend to the Isle of Man—

(a) paragraphs 200N and 205 of Schedule 18;
(b) sections 204(1), 205(1) and 206, so far as relating to those paragraphs.”

See the explanatory statement for amendment 227. Paragraph 200N in amendment 222 amends the Competition Act 2006 (Extension of Takeover Panel Provisions) (Isle of Man) Order 2008.—(Margot James.)

Clause 207, as amended, ordered to stand part of the Bill.

Clause 208

SHORT TITLE

Amendment made: 75, in clause 208, page 121, line 24, leave out subsection (2)

This amendment removes the privilege amendment inserted by the Lords.—(Margot James.)

Clause 208, as amended, ordered to stand part of the Bill.

New Clause 1

REPRESENTATION OF DATA SUBJECTS WITH THEIR AUTHORITY: COLLECTIVE PROCEEDINGS

'(1) The Secretary of State may by regulations make provision for representative bodies to bring proceedings before a court or tribunal in England and Wales or Northern Ireland combining two or more relevant claims.

(2) In this section, “relevant claim”, in relation to a representative body, means a claim in respect of a right of a data subject which the representative body is authorised to exercise on the data subject’s behalf under Article 80(1) of the GDPR or section 183.

(3) The power under subsection (1) includes power—

(a) to make provision about the proceedings;
(b) to confer functions on a person, including functions involving the exercise of a discretion;
(c) to make different provision in relation to England and Wales and in relation to Northern Ireland.

(4) The provision mentioned in subsection (3)(a) includes provision about—

(a) the effect of judgments and orders;
(b) agreements to settle claims;
(c) the assessment of the amount of compensation;
(d) the persons to whom compensation may or must be paid, including compensation not claimed by the data subject;
(e) costs.

(5) Regulations under this section are subject to the negative resolution procedure.”

This new clause confers power on the Secretary of State to make regulations enabling representative bodies (defined in Clause 183) to bring collective proceedings in England and Wales or Northern Ireland combining two or more claims in respect of data subjects’ rights.—(Margot James.)

Brought up, read the First and Second time, and added to the Bill.

New Clause 2

DUTY TO REVIEW PROVISION FOR REPRESENTATION OF DATA SUBJECTS

'(1) Before the end of the review period, the Secretary of State must—

(a) review the matters listed in subsection (2) in relation to England and Wales and Northern Ireland,
(b) prepare a report of the review, and
(c) lay a copy of the report before Parliament.

(2) Those matters are—

(a) the operation of Article 80(1) of the GDPR,
(b) the operation of section 183,
(c) the merits of exercising the power under Article 80(2) of the GDPR (power to enable a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise some or all of a data subject’s rights under Articles 77, 78 and 79 of the GDPR without being authorised to do so by the data subject), and
(d) the merits of making equivalent provision in relation to data subjects’ rights under Article 82 of the GDPR (right to compensation).

(3) “The review period” is the period of 30 months beginning when section 183 comes into force.

(4) After the report under subsection (1) is laid before Parliament, the Secretary of State may by regulations—

(a) exercise the powers under Article 80(2) of the GDPR in relation to England and Wales and Northern Ireland, and
(b) make provision enabling a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise a data subject’s rights under Article 82 of the GDPR in England and Wales and Northern Ireland without being authorised to do so by the data subject.

(5) The powers under subsection (4) include power—

(a) to make provision enabling a data subject to prevent a body or other organisation from exercising, or continuing to exercise, the data subject’s rights;
(b) to make provision about proceedings before a court or tribunal where a body or organisation exercises a data subject’s rights,
(c) to make provision for bodies or other organisations to bring proceedings before a court or tribunal combining two or more claims in respect of a right of a data subject,
(d) to confer functions on a person, including functions involving the exercise of a discretion;
(e) to amend sections 164 to 166, 177, 183, 196, 198 and 199;
(f) to insert new sections and Schedules into Part 6 or 7;
(g) to make different provision in relation to England and Wales and in relation to Northern Ireland.

(6) The provision mentioned in subsection (5)(b) and (c) includes provision about—

(a) the effect of judgments and orders;
(b) agreements to settle claims;
(c) the assessment of the amount of compensation;
New Clause 5

BILL OF DATA RIGHTS IN THE DIGITAL ENVIRONMENT

Schedule [Bill of Data Rights in the Digital Environment] shall have effect.

This new clause would introduce a Bill of Data Rights in the Digital Environment.—(Liam Byrne.)

Brought up, and read the First time.

Liam Byrne (Birmingham, Hodge Hill) (Lab): I beg to move, That the clause be read a Second time.

The Chair: With this it will be convenient to discuss the following:

New clause 6—

“Bill of Data Rights in the Digital Environment (No. 2)

(1) The Secretary of State shall, by regulations, establish a Bill of Data Rights in the Digital Environment.

(2) Before making regulations under this section, the Secretary of State shall—

(a) consult—

(i) the Commissioner,

(ii) trade associations,

(iii) data subjects, and

(iv) persons who appear to the Commissioner or the Secretary of State to represent the interests of data subjects; and

(b) publish a draft of the Bill of Rights.

(3) The Bill of Data Rights in the Digital Environment shall enshrine—

(a) a right for a data subject to have privacy from commercial or personal intrusion,

(b) a right for a data subject to own, curate, move, revise or review their identity as founded upon personal data (whether directly or as a result of processing of that data),

(c) a right for a data subject to have access to their data profiles or personal data protected, and

(d) a right for a data subject to object to any decision made solely on automated decision-making, including a decision relating to education and employment of the data subject.

(4) Regulations under this section are subject to the affirmative resolution procedure.”

This new clause would empower the Secretary of State to introduce a Bill of Data Rights in the Digital Environment.

New Schedule 1

Bill of Data Rights in the Digital Environment

The UK recognises the following Data Rights:

Article 1 — Equality of Treatment

1 Every data subject has the right to fair and equal treatment in the processing of his or her personal data.

Article 2 — Security

1 Every data subject has the right to security and protection of their personal data and information systems.

Article 3 — Free Expression

1 Every data subject has the right to deploy his or her personal data in pursuit of their fundamental rights to freedom of expression, thought and conscience.

Article 4 — Equality of Access

1 Every data subject has the right to access and participate in the digital environment on equal terms.

Article 5 — Privacy

1 Every data subject has right to respect for their personal data and information systems and as part of his or her fundamental right to private and family life, home and communications.

Article 6 — Ownership and Control

1 Every data subject is entitled to know the purpose for which personal data is being processed or his or her right to ownership. Government, corporations and data controllers must obtain meaningful consent for use of people’s personal data.

Article 7 — Algorithms

1 Every data subject has the right to transparent and equal treatment in the processing of his or her personal data by an algorithm or automated system.

Article 8 — Participation

1 Every data subject has the right to deploy his or her personal data and information systems to communicate in pursuit of the fundamental right to freedom of association.

Article 9 — Protection

1 Every data subject has the right to safety and protection from harassment and other targeting through use of personal data whether sexual, social or commercial.

Article 10 — Removal

1 Every data subject is entitled to revise and remove their personal data.

Compensation

Breach of any right in this Bill will entitle the data subject to fair and equitable compensation under existing enforcement provisions. If none apply, the Centre for Data Ethics will establish and administer a compensation scheme to ensure just remedy for any breaches.

Application to Children

1 The application of these rights to a person less than 18 years of age must be read in conjunction with the rights set out in the United Nations Convention on the Rights of the Child.

1 Where an information society service processes data of persons less than 18 years of age it must do so under the age appropriate design code.”

Liam Byrne: We now come to the good stuff. Members of the Committee can look forward to an enormous amount of ground to cover in the debates ahead. We will try to speed through it as quickly as we can, but there is an awful lot of ground to cover. New clauses 5 and 6 and new schedule 1, tabled in my name and that of my hon. Friends, are an attempt to provoke the Government into being more ambitious in their strategy for the digital world. Every so often, as a great nation, we make important declarations of rights.
Rights are important because they ensure that progress is democratised, but they also provide important new protections against new imbalances of power that arise. We really began to turn our minds to this about 803 years ago when we came up with Magna Carta. We then made a much more sweeping and important statement that received Royal Assent on 16 December 1689. We had a couple of centuries off and in more recent years we went rights crazy and started signing universal declarations in the years after the second world war with much greater speed. We had the universal declaration of human rights, in which British civil servants took a leading role; the UN convention on the rights of the child; the charter of fundamental rights, which we helped shape; and the incorporation of those regimes of rights, which we wrote for our neighbours, into British law through the Human Rights Act 1998 and the Equality Act 2010.

Over the years, the regime of rights that we have pioneered in this country has been absolutely fundamental to the progress that we have made as a nation. If we go back to the debates here in the 1630s and 1640s, we see that the rights of new entrepreneurs to defend the wealth that they had created through trading, particularly in the Atlantic colonies—examples include the Virginia Company and, later, the East India Company—and the rights that we sought to enshrine and protect against arbitrary taxation, were absolutely fundamental in laying the foundation for the industrial revolution that really began to take off in the years after the Bill of Rights was enshrined by William III in 1689.

The argument that I want to make this morning is that the sweeping changes of the digital age mean that it would be wise of us to consider a similarly ambitious set of rights for the digital age. Anyone who has an interest in economic history will know that, ultimately, we can never contract for anything. Ultimately, a handshake will always be as important as a contract, and a handshake relies on an environment of trust. When countries do not have environments of trust, they lack economic institutions that allow their economies to flourish.

The challenge in this country today is that we are not making quite as much progress with the digital economy as perhaps we could be. Indeed, in most international indexes, where we should be at the top, we are normally batting at about fifth and sixth. That is not terrible, but most of us would like it to be better. We are at the home of the scientific revolution and the industrial revolution. We should be at the top of the table, not fifth and sixth.

That provokes us to ask what is the state of online trust and digital trust in this country. The figures that I have dug out are for the time before the scandals that we have learned about over the last couple of weeks, which will not have put trust levels up. Online fraud is now growing very quickly. In fact, Action Fraud says that 70% of all fraud is now cyber-enabled. That is not simply a commercial problem; it is also a public sector problem. Public services such as the NHS hold vast quantities of public data. The NHS has been hit very badly by malware in a way that has provoked real questions about the UK’s digital resilience. The National Audit Office said that the NHS and the then Department of Health must “get their act together” or suffer far worse than the chaos of 2017. Edelman recently produced a survey that said that one quarter of the UK population trusts social media and 61% trust traditional media, so there are huge imbalances in what people trust today.

I have been interested in this question for a while, and I have been interested in seeing what we can learn from some of the world’s digital leaders. On a recent visit to Estonia, which is by some agreement the world’s leading digital society, the thing that really struck me was the fact that digital trust is supremely high. The Government of Estonia took the big decision, when they left that north-west corner of the USSR, that they would have to take a big gamble on the future. As we leave the north-west corner of Europe, we need to be taking a similar big bet on the future. We need to be betting on digital in the way we bet on steam a couple of centuries ago.

Two things are absolutely key to the digital environment in Estonia. One is a platform called X-Road, which allows Government data from distributed databases to come together to answer particular kinds of problems, but absolutely fundamental is the public option of an e-ID scheme. That involves two-factor authentication and it comes with important features such as the ability for people to look online at who has been using their data, who has been accessing it, and what they have been using it for. In fact, doctors and police officers have gone to jail because they have misused their ability to access online records—medical records, for instance.

Anyone in this country who has tried to file their taxes online, as I did early in January, will know that the Government gateway here is nowhere near that level. Once I had been issued with my fifth online ID, I frankly gave up and rang the MPs’ hotline, and the person there said, “Yeah, we’ve had lots of problems like this. You can just file your tax return on paper like everybody else.” We are sadly lacking the kind of digital infrastructure that many other countries enjoy.

The point about the public option for electronic ID is that there is a country that has decided that the right to a secure ID is a fundamental right, and on that fundamental right has flourished a digital economy that has helped to create the world’s leading digital society. There are now 3,000 Government e-services and 5,000 private sector e-services that sit on top of that platform. When I met the former Prime Minister of Estonia, he said that the key to winning the argument was that financial institutions such as banks were so confident in the public infrastructure that had been created that they were prepared to go out to the public in Estonia and say, “The public option for an electronic ID is the right option.”

12.30 pm

Think about how many different IDs and passwords we have. Think about the complexity and the risk that creates. We have no idea who is using all that data. The point is that if we have a secure regime of trust, it will become possible for a private sector to flourish in a new way. That is why we think having a much more comprehensive bill of digital rights—or a bill of data rights, as we have had to call it to get it in scope—is compelling, and we would like the Government to consider it.

This is not just about the new freedoms that we might want guaranteed by these new rights. There is also the question of the new protections we might want from them.
Matt Warman (Boston and Skegness) (Con): I am enjoying the right hon. Gentleman's history lesson about Estonia.

Liam Byrne: There is lots more of it.

Matt Warman: I had that sense. The key thing about Estonia, aside from the fact that it is a far, far smaller country, is that the register for the digital ID that the right hon. Gentleman is talking about is held centrally by the Government. There is a fundamental difference between this country and Estonia. If he were seriously to propose to citizens in the UK that the Government should hold that central register, I think they would give him pretty short shrift. In his long lecture, will he either make the case for a Government-held central register or acknowledge that it would still be a pretty tough thing to get past the British public?

Liam Byrne: I am very happy to. I am lucky enough to be able to draw on my extensive experience as the Minister for ID cards in the Labour Government. I will take the hon. Gentleman, in detail, through the architecture I proposed. Well, he asked for it.

The challenge we confronted in about 2006 is that we originally proposed one big database for all the data, including biometric data. That was an error. The architecture I proposed in its stead was a way of connecting three different databases—one that would have basically held Driver and Vehicle Licensing Agency data, a second that would have held the passport services data, and then a couple of identifiers that would have allowed those two records to be indexed and joined together. That brought the cost of the ID card system down by about two thirds.

Although the hon. Member for Boston and Skegness says that the British public would not like Government databases to hold all that information, that happens to be the country they live in. The Passport Office and DVLA hold comprehensive data on most people, and people find that extremely useful.

I was very careful about what I said. What I said was not that we should have compulsory e-ID, but that we should have a public option so people can choose to use it. That is obviously a different regime from Estonia’s, where ID cards have been compulsory since the country was invented about a century ago.

Giving people a public option would be quite attractive. There are, however, important safeguards that we need to learn from. It would be a mistake to have biometric information connected to that kind of service. We do not need biometric information connected to that kind of service. The ID card system in India has gone down that route, and it has suffered pretty significant leaks of biometric data over the past year and a half. If people get their hands on that data, that will be far more dangerous. The Estonian system, in which people have an electronic ID and a password that sits in their head—a two-factor authentication—has proven much more successful.

My broader point is that we should have a debate about the data rights that we, as citizens of this country, should have. Partly, that is about having rights to things that would make our lives better and would allow us to pursue new freedoms, such as the freedom not to have a million and one passwords, which we lose track of. It is also about having certain protections. We have had a useful debate, and will have an even longer one shortly, about the right to be treated fairly by algorithms. That is obviously incredibly important. The Government have given a nod in that direction, so the Minister will probably say a little about their digital charter.

On the different sides of the House, there are different philosophies on rights. The Conservative party traditionally defends rights to do with negative freedoms, and my side often talks the language of positive freedoms—the power to do things, which we think is necessary for social justice. However, I hope that in the months ahead we can have a sensible conversation about what negative and positive freedoms we can crystallise and enshrine in a bill of digital rights. At some point in this century, we shall write that. It is inevitable, because the world will change in a way that requires it, and the citizens of this country will begin to demand it. What we are starting to debate today will come to pass at some point. I hope to be the Minister who drives it through in the next Labour Government, which is imminent.

I hope, too, that we can debate that idea and help to perfect it. Where regimes of rights have been most effective, they have stood the test of time. For something to stand the test of time, it always helps if there is a little—not too much—cross-party consensus.

The new schedule has a couple of ideas at its core, and we are lucky in having been able to draw on not only the rights literature, but the incredible work of Baroness Kidron. As well as being a talented member of the creative industries, she has been one of the leading champions of the creation of strong digital rights for our children. As we have rehearsed in Committee previously, the issue is fundamental, not marginal. About a third of online users are children. The Government will have, in a way, to step in that direction. They will have to step towards new clauses 5 and 6, and new schedule 1, because they have committed to issuing an age-appropriate design code that will operationalise clause 124. I want to encourage the Government to think creatively about the way they will write the code of practice on age-appropriate design codes, with at least one eye on the broader bill of data and digital rights, which we want to propose.

The 5Rights movement has a couple of important ideas. One is the right to remove: children should be able to remove content that they have uploaded. There are probably members of the Committee who have posted all kinds of unfortunate content in their lives, which they might not want to have there in the future. That is certainly true of many children I know. The right to remove is, I think, widely accepted, and is reflected as one of the ambitions of the Bill.

The second right is the right to know. Children should be able to learn easily the who, what and why—and know for what purposes their data is being exchanged. That is important. The Minister herself has talked about the need to educate online users—to educate us all so that we become better critical consumers of the content that we find online. That is doubly important for children.

The third right is the right to safety and support. Much of what upsets young people online is not illegal. It is legal. Support is often quite sparse and fragmented. It is often pretty invisible to children and young people when they need it most.
It will be challenging for the Government to turn the right to informed and conscious use into part of the code of practice, but that is incredibly important. It is simply unfortunate that social media firms spend quite so much money, effort and engineering talent on creating features that create a kind of addiction because of the rush of endorphins that they trigger in young people’s minds.

Those technologies, techniques and tricks of the trade are based on exactly the same principles as casino slot machines, and it is quite telling that a number of social media leaders have, over the last six months, gone on the record to say that they will not let their children use the apps that millions of children around the world use. The right to informed and conscious use will be difficult for the Government to interpret, but it is none the less important.

The right to digital literacy is perhaps the most important of all. It is something that our schools already do a terrific job of putting into practice, but what struck me in Estonia is the way that people see the right to internet access as basically a social right. That is surely something that we should debate and put in practice, too.

We have had quite a collection of evidence over the last year from people such as the Children’s Commissioner, who have ridden in behind and supported Baroness Kidron’s 5Rights movement. The Children’s Commissioner recently said:

“The social media giants have simply not done enough to make children aware of what they are signing up to when they install an app or open an account.”

The idea that children can look at these pages and pages of terms and conditions and just click and agree to them is obviously nonsensical. Indeed, the Children’s Commissioner, when reflecting on that, said:

“Children have absolutely no idea that they are giving away the right to privacy or the ownership of their data or the material they post online.”

The Government have obviously sought to exercise their derogation under the GDPR and set the age of consent at 13, rather than 16, so the code of practice that the Minister has agreed to is really important.

We would like this bill of data rights to go alongside more effective mechanisms to ensure that those rights are enforceable. That is why we tabled our amendments to clause 80(2). We think it is impossible in today’s economic environment for ordinary citizens to take effective action against the biggest firms on earth. These five firms have a market capitalisation, although it is slightly less than it was, of about $2.5 trillion, so the idea that a humble citizen can take on some of these giants is nonsensical. We would therefore like this bill of data rights to sit alongside a much more effective, open and democratic form of class action.

I am really interested in the Minister’s observations on the rights we have set out. Article 1 of our proposed new schedule covers equality of treatment, which is enshrined in the GDPR. The GDPR is long—we have made incredible progress through it, article by article—and it is a miracle that we have arrived at page 123 of the Bill by Thursday afternoon, but that is a real testament to the skilful chairing of Mr Hanson and you, Mr Streeter. The principle of equality of treatment is written throughout every clause of the Bill. The point is that it is written through 200 clauses, so we think a basic statement of equality of treatment is a good place to start.

Article 2 covers the right to security, which is the subject of the Bill. Again, let us set that out in terms. Article 3 covers the right to free expression, which is something we have signed up to in articles of the European convention on human rights. It is something that we should set within the context of a bill of data rights. Article 4 covers the right of equality of access. Giving equal access to the digital environment is extremely important. The digital environment creates a network, and network effects mean that the more people joined to it, the greater the value of the network. It is important to specify, set out and declare that we see equality of access to the digital environment as important.

Article 5 sets out the right to privacy, which, again, is scattered throughout the Bill, although we would like to consolidate and crystalise it and bring it together. Article 6 covers ownership and control, which will only grow in importance. This is not the place to get into the vexed debate about who owns the copyright to the data that someone might have and the new data that might be created by joining that data with someone else’s. However, the question of who owns the copyright, and therefore who owns the value of data that is personal in origin, is only going to grow. That debate is almost the 21st century equivalent to that on the enclosure of the commons, frankly. Who owns the copyright of data will become more important as the value of data grows exponentially.

Article 7 talks about the right to fairness when it comes to automated decision making, which we will come to in the debate on algorithmic fairness. Algorithms are making more and more decisions in our lives. People have a right not to be treated unfairly as a result of those decisions. In the phrase used by my hon. Friend the Member for Cambridge, we cannot have a world in which yesterday’s injustice is hard-coded into tomorrow’s injustice. We think that ensuring a right to algorithmic fairness in our bill of data rights is important. The rights to participation, protection and removal are important too.

We have a long tradition of rights in this country; we are the world’s pioneers of them. It is because we have been that pioneer down the centuries that we are today the world’s fifth-biggest economy, but we are not the world’s leading digital society. It is an ambition of the Opposition that we should be, and we think that a bill of digital rights would help us to get there.

12.45 pm

Darren Jones (Bristol North West) (Lab): I welcome new schedule 1, in the name of my right hon. Friend the Member for Birmingham, Hodge Hill and my hon. Friend the Member for Ogmore and for Sheffield, Heeley. I should declare that I was first on Facebook as a 19-year-old. Now, as a 31-year-old, I can declare that I do not think there is anything on there that I am embarrassed of.

Gareth Snell (Stoke-on-Trent Central) (Lab/Co-op): Lucky you.

Darren Jones: I reserve the right for other hon. Friends to remove content from their social media.
Returning to the issue of health data, I have personal views about how we might tax revenues from platforms in a better way. I welcome the comments made by the Chancellor of the Exchequer, in line with his counterparts in Europe, about looking at how we tax revenues where they are made, not where the company is headquartered. That is a positive move, but surely if all this NHS data is creating profits for other companies and organisations, we can create a situation in which patients also benefit from that, by sharing in the profits that are made and by seeing value redirected into the health service.

All that becomes anchored in the question of ownership. There is still this legal space that says that data subjects do not own their own data. We need a much broader debate on that. [ Interruption. ] Members are shaking their heads. I am happy to take interventions, if Members would like.

**Liam Byrne:** Will my hon. Friend reflect on the idea that if someone is genuinely a popular capitalist and believes in the distribution of wealth as the basis of economic growth, then recognising and crystallising the value of personal data is actually pro-growth?

**Darren Jones:** I agree entirely. I confess I never got all the way through my version of Piketty, but the idea of value through assets, as opposed to through the stagnating wages in our economy today, plays into this conversation around data. People from poorer backgrounds may not inherit houses or land, but they create their own data every day. It is an asset that should belong to them. They should be able to share in its value when companies around the world are making enormous profits off the back of it. In this digital age, there is a huge call for equality of opportunity and equality of access. We need to try to get those right in these fundamental understandings of the digital market and the rights that exist around it.

Lastly, I encourage and strengthen my right hon. Friend’s arguments on the application of these principles to children. The Committee has already debated how parental consent is not needed after the age of 13. One of my early jobs as legal counsel at BT was the dubious task of consolidating terms and conditions. Hon. Members who are no doubt happy customers of BT, with perhaps broadband, TV and sport, would originally have had to read five or six different documents that were very long and complicated. I had to consolidate those. That was not good enough, so I commissioned a YouTube star to do a video, which can be seen on the terms and conditions page, to try to explain some of these things. Even for adults, this was a really hard and laborious task.

I am not saying that it is for Government to tell businesses how to communicate to children. Second Reading and some of the Committee’s debates show—dare I say it—that we are probably not best placed to have those conversations. However, it is really important that there is an expectation on businesses that they take steps to ensure that children are properly engaged and really understand what they are signing up to, especially as the Government have opted to go to the minimum range for consent, going to 13.

I just wanted to re-emphasise the debate on ownership and on children. I support my right hon. Friend’s new schedule and new clauses, and I hope the Government will support them.
Margot James: My response will encompass our digital charter, as the right hon. Member for Birmingham, Hodge Hill mentioned, and I will also answer some of the points he made in his interesting exposition of his rights-based approach. I agree with him: the internet is a powerful force for good, serving humanity and spreading ideas, freedom and opportunity across the world. Yet, as he rightly states, there are considerable trust issues, which can have only worsened in recent days.

I would like to emphasise the point made by my hon. Friend the Member for Gordon that the UK has a strong digital economy accounting for over 12.5% of GDP, which makes us the leading digital economy in the G20.

The right hon. Gentleman was critical of Government sites and services, but we have developed a system that is being taken up by several other countries, including New Zealand, which are adopting our approach to providing Government services online. I am sorry that his experience on the tax side was not great, and there are always exceptions, but on the whole we are leaders in the provision of Government services online.

Citizens rightly want to know that they will be safe and secure online. Tackling these challenges in an effective and responsible way is absolutely critical. The digital charter is our response. It is a rolling programme of work to agree norms and rules for the online world and to put them into practice. In some cases, that will be through shifting expectations of behaviour and resetting a settlement with internet companies. In some cases, we will need to agree completely new standards; in others, we will want to update our laws and regulations. Our starting point is that we expect the same rights and behaviour online as we do offline, with the same ease of enforcement.

The charter’s core purpose is to make the internet work for everyone—for citizens, businesses and society as a whole—and it is based on liberal values. Every country is grappling with these challenges. The right hon. Gentleman suggested last week that the Government are not averse to making declaratory statements of rights and interpreting them into law, but his key example related to human rights. The Human Rights Act provides a detailed and well-considered legislative framework for those rights and ensures that they are meaningful.

Liam Byrne: When the right hon. Member for Surrey Heath (Michael Gove), who is now the Secretary of State for Environment, Food and Rural Affairs, was Secretary of State at the Ministry of Justice, he launched a consultation about an English Bill of Rights, which was about not simply about human rights but a much broader set of rights. I do not think there is a big difference in our approaches to rights. Actually, I think there is a shared approach, as has been recognised down the years.

Margot James: Yes, much of our approach is shared. The Government decided not to proceed with that Bill of Rights, but the right hon. Gentleman rightly points out that both our parties have a keen interest in this area. However, to set out his proposed bill of data rights in primary legislation would cut across the GDPR. It would impose its own rights of rectification and erasure, its own notion of control and its own obligations on controllers to keep data secure, but, of course, the GDPR already does that, and comparable rights are provided for in the Bill. I am concerned about how the Commission would react to such an attempt to redefine data protection standards. That is one of our main concerns with his new clauses and new schedule, no matter how much we might agree with the sentiments behind them. Given that, and the fact that we are proceeding with our digital charter, I feel that the Bill, in essence, covers this issue, and I need say no more about it.

Liam Byrne: Our proposed bill of data rights seeks not to redefine but to enshrine, so the rights reflected in the GDPR are no more than enshrined in it. The point is that it would go over and above the rights and obligations set out in this Bill. The right of equal access to the internet, the crystallisation of the right to expression and the advancement of the debate about the right to data ownership are important provisions whose time will come. At some point, due to the way the world is changing, our citizens and constituents will begin to demand both a democratisation of the privileges of this new age and of progress, and the right to effective defences and new protections.

I am glad that the Minister agrees with the sentiment behind the new clause, and I recognise that she perhaps does not see this Bill as the place to consolidate our brilliant ideas into the law of the land. I listened with interest to what she said about a rolling programme of ideas in the digital charter. There is a challenge with that approach: it will end up following the cones hotline model of public service reform. It will not live or sing; it will be bedevilled by voluntary codes, bureaucracy and operational procedures, and it will end up not really making a difference to the world. Our bill of data rights is clear.

If rights are to be a reality, they need not to be a mystery but to be understood. They need to be something that people can talk about in a pub. They need to be something not that is set out in 250 pages of primary legislation but that can be set out on the back of a fag packet. In our bill of data rights, we set out a clear agenda that would make a difference and be easily understood and enforced. It would be an improvement and would take forward the rights and liberties of the citizens of this country.

The Chair: Does the right hon. Gentleman wish to press the new clause to a vote?

Liam Byrne: No. I beg to ask leave to withdraw the clause.

Clause, by leave, withdrawn.
Ordered, That further consideration be now adjourned. 
—(Nigel Adams.)

1 pm
Adjourned till this day at Two o’clock.
CONTENTS

New clauses considered.
Bill, as amended, to be reported.
No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Monday 26 March 2018
The Committee consisted of the following Members:

**Chairs:** David Hanson, †Mr Gary Streeter

† Adams, Nigel (Lord Commissioner of Her Majesty's Treasury)
† Atkins, Victoria (Parliamentary Under-Secretary of State for the Home Department)
† Byrne, Liam (Birmingham, Hodge Hill) (Lab)
† Clark, Colin (Gordon) (Con)
† Elmore, Chris (Ogmore) (Lab)
Haigh, Louise (Sheffield, Heeley) (Lab)
† Heaton-Jones, Peter (North Devon) (Con)
† Huddleston, Nigel (Mid Worcestershire) (Con)
† Jack, Mr Alister (Dumfries and Galloway) (Con)
† James, Margot (Minister of State, Department for Digital, Culture, Media and Sport)

† Jones, Darren (Bristol North West) (Lab)
† Lopez, Julia (Hornchurch and Upminster) (Con)
† McDonald, Stuart C. (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP)
Murray, Ian (Edinburgh South) (Lab)
† O'Hara, Brendan (Argyll and Bute) (SNP)
† Snell, Gareth (Stoke-on-Trent Central) (Lab/Co-op)
† Warman, Matt (Boston and Skegness) (Con)
† Wood, Mike (Dudley South) (Con)
† Zeichner, Daniel (Cambridge) (Lab)

Kenneth Fox, Committee Clerk

† attended the Committee
Public Bill Committee

Thursday 22 March 2018

(Afternoon)

[Mr Gary Streeter in the Chair]

Data Protection Bill [Lords]

New Clause 7

Application of Equality Act (Services and Public Functions)

“(1) Part 3 (Services and public functions) of the Equality Act 2010 (‘the Equality Act’) shall apply to the processing of personal data by an algorithm or automated system in making or supporting a decision under this section.

(2) A ‘decision’ in this section means a decision or any part of a decision that engages a data subject (D)’s rights, freedoms or legitimate interests concerning—

(a) the provision of services to the public and

(b) the exercise of public functions by a service-provider.

(3) Nothing in this section detracts from other rights, freedoms or legitimate interests in this Act, the Equality Act or in any other primary or secondary legislation relating to D’s personal data, employment, social security or social protection.”—(Liam Byrne)

This new clause would apply Part 3 of the Equality Act 2010 to the processing of personal data by an algorithm or automated system or supporting a decision under this new clause.

Brought up, and read the First time.

2 pm

Liam Byrne (Birmingham, Hodge Hill) (Lab): I beg to move, That the clause be read a Second time.

The Chair: With this it will be convenient to discuss the following:

New clause 8—Application of the Equality Act (Employment)

“(1) Part 5 (Employment) of the Equality Act (‘the Equality Act’) shall apply to the processing of personal data by an algorithm or automated system in making or supporting a decision under this section.

(2) A ‘decision’ in this section means a decision that engages a data subject (D)’s rights, freedoms or legitimate interests concerning—

(a) recruitment,

(b) the terms and conditions of employment,

(c) access to opportunities for promotion, transfer or training, and

(d) dismissal.

(3) Nothing in this section detracts from other rights, freedoms or legitimate interests in this Act, the Equality Act or in any other primary or secondary legislation relating to D’s personal data, employment, social security or social protection.”

This new clause would apply Part 5 of the Equality Act 2010 to the processing of personal data by an algorithm or automated system or supporting a decision under this new clause.

New clause 9—Right to algorithmic fairness at work

“(1) A person (‘P’) has the right to fair treatment in the processing of personal data by an algorithm or automated system in making a decision under this section.

(2) A “decision” in this section means a decision in which an algorithm or automated system is deployed to support or make a decision or any part of that decision that engages P’s rights, freedoms or legitimate interests concerning—

(a) recruitment,

(b) the terms and conditions of employment,

(c) access to opportunities for promotion, transfer or training, and

(d) dismissal.

(3) “Fair treatment” in this section means equal treatment between P and other data subjects relevant to the decision made under subsection (2) insofar as that is reasonably practicable with regard to the purpose for which the algorithm or automated system was designed or applied.

(4) In determining whether treatment of P is “fair” under this section the following factors shall be taken into account—

(e) the application of rights and duties under equality and other legislation in relation to any protected characteristics or trade union membership and activities,

(f) whether the algorithm or automated system has been designed and trained with due regard to equality of outcome,

(g) the extent to which the decision is automated,

(h) the factors and weighting of factors taken into account in determining the decision,

(i) whether consent has been sought for the obtaining, recording, using or disclosing of any personal data including data gathered through the use of social media, and

(j) any guidance issued by the Centre for Data Ethics and Innovation.

(5) “Protected characteristics” in this section shall be the protected characteristics defined in section 4 of the Equality Act 2010.”

This new clause would create a right to fair treatment in the processing of personal data by an algorithm or automated system in making a decision regarding recruitment, terms and conditions of employment, access to opportunities for promotion etc. and dismissal.

New clause 10—Employer’s duty to undertake an Algorithmic Impact Assessment

‘(1) An employer, prospective employer or agent must undertake an assessment to review the impact of deploying the algorithm or automated system in making a decision to which subsection (1) of section [Application of Equality Act (Employment)] applies [an ‘Algorithmic Impact Assessment’].

(2) The assessment undertaken under subsection (1) must—

(a) identify the purpose for which the algorithm or automated system was designed or applied,

(b) test for potential discrimination or other bias by the algorithm or automated system,

(c) consider measures to advance fair treatment of data subjects relevant to the decision, and

(d) take into account any tools for Algorithmic Impact Assessment published by the Centre for Data Ethics and Innovation.”

This new clause would impose a duty upon employers to undertake an Algorithmic Impact Assessment.

New clause 11—Right to an explanation

“(1) A person (‘P’) may request and is entitled to be provided with a written statement from an employer, prospective employer or agent giving the following particulars of a decision to which subsection (1) of section [Right to algorithmic fairness at work] applies—

(a) any procedure for determining the decision,

(b) the purpose and remit of the algorithm or automated system deployed in making the decision,

(c) the criteria or other meaningful information about the logic involved in determining the decision, and

(d) the factors and weighting of factors taken into account in determining the decision.

(2) A ‘decision’ in this section means a decision in which an algorithm or automated system is deployed to support or make a decision or any part of that decision that engages P’s rights, freedoms or legitimate interests concerning—

(a) recruitment,

(b) the terms and conditions of employment,

(c) access to opportunities for promotion, transfer or training, and

(d) dismissal.

(3) Nothing in this section detracts from other rights, freedoms or legitimate interests in this Act, the Equality Act or in any other primary or secondary legislation relating to D’s personal data, employment, social security or social protection.”
the implications of automated decision making, which are of machine learning. Along with Ben Jaffey QC, a couple of points after the afternoon, but, none the less, I want to tease out a hear that I am not going to read through that this provoking report. The Committee will be frustrated to W ork commission, which produced a long, thought-clauses is rooted in the excellent work of the Future of constituents in this new world.

The growth in decisions that are made through automated decision making has been exponential, and there are decision making has been unaccountable and highly sophisticated automated or semi-automated systems are now making decisions that bear on fundamental elements of people’s work, including recruitment, pay and discipline. Just today, I was hearing about the work practices at the large Amazon warehouse up in Dundee. I think, where there is in effect digital casualisation. Employees are not put on zero-hours contracts, but they are put on four-hour contracts. They are guided around this gigantic warehouse by some kind of satnav technology on a mobile phone, but the device that guides them around the warehouse is also a device that tracks how long it takes them to put together a basket.

That information is then arranged in a nice league table of employees of who is the fastest and who is slowest, and decisions are then taken about who gets an extension to their contracted hours each week and who does not. That is a pretty automated kind of decision. My hon. Friend the Member for Eltham (Clive Efford) was describing to me the phenomenon of the butty man—the individual who decided who on a particular day got to work on the docks or on the construction site. In the pub at the end of the week, he divvied up the winnings and decided who got what, and who got what the following week. That kind of casualisation is now being reinvented in a digital era and is something that all of us ought to be incredibly concerned about.

What happens with these algorithms is called, in the jargon, socio-technical—what results is a mixture of conventional software, human judgment and statistical models. The issue is that very often the decisions that are made are not transparent, and are certainly not open to challenge. They are now quite commonly used by employers and prospective employers, and their agents, who are able to analyse very large datasets and can then deploy artificial intelligence and machine learning to make inferences about a person. Quite apart from the ongoing debates about how we define a worker and how we define employment—the subject of a very excellent report by my old friend Matthew Taylor, now at the RSA—there are real questions about how we introduce new safeguards for workers in this country.

I want to highlight the challenge with a couple of examples. Recent evidence has revealed how many recruiters use—surprise, surprise—Facebook to seek candidates in ways that routinely discriminate against older workers by targeting advertisements for jobs in a particular way. Slater and Gordon, which is a firm of excellent employment lawyers, showed that about one in five company executives admit to unlawful discrimination when advertising jobs online. The challenge is that when jobs are advertised in a targeted way, by definition they are not open to applicants from all walks of life, because lots of people just will not see the ads.

Women and those over the age of 50 are now most likely to be prevented from seeing an advert. Some 32% of company executives say that they have discriminated against those who are over 50, and a quarter have discriminated in that way against women. Nearly two thirds of executives with access to a profiling tool have said that they use it to actively seek out people based on criteria as diverse as age, gender and race. If we are to deliver a truly meritocratic labour market, where the rights of us all to shoot for jobs and to develop our skills and capabilities are protected, and who get work practices have to stop. If we are to stop them, the law needs to change, and it needs to change now.
This battery of new clauses sets out to do five basic things. First, they set out some enhancements and refinements to the Equality Act 2010, in a way that ensures that protection from discrimination is applied to new forms of decision making, especially when those decisions engage core rights, such as rights on recruitment, terms of work, or dismissal. Secondly, there is a new right to algorithmic fairness at work, to ensure equal treatment. Thirdly, there is the right to an explanation when a decision is taken in a way that affects core elements of work life, such as a decision to hire, fire or suspend someone. Fourthly, there is a new duty for employers to undertake an algorithmic impact assessment, and fifthly, there are new, realistic ways for individuals to enforce those rights in an employment tribunal. It is quite a broad-ranging set of reforms to a number of different parts of legislation.

Daniel Zeichner (Cambridge) (Lab): My right hon. Friend is making a powerful case about the importance of the Equality Act in respect of the Bill, but may I offer him another example? He mentioned the case of Mark, who was a university lecturer who was made redundant because of his age. The Act sets out a number of remedies for those who have been discriminated against in that way, but it is not clear how the Bill proposes to correct that sin. Injustices in the labour market are multiplying, and there is a cross-party consensus for a stronger defence of workers. In fact, the Member of Parliament for the town where I grew up, the right hon. Member for Harlow (Robert Halfon), has led the argument in favour of the Conservative party rechristening itself the Workers’ party, and the Labour party was founded on a defence of labour rights, so I do not think this is an especially contentious matter. There is cross-party consensus about the need to stand up for workers’ rights, particularly when wages are stagnating so dramatically.

We are therefore not divided on a point of principle, but the Opposition have an ambition to do something about this growing problem. The Bill could be corrected in a way that made a significant difference. There is not an argument about the rights that are already in place, because they are enshrined in the Equality Act, with which Members on both sides of the House have agreed. The challenge is that the law as it stands is deficient and cannot be applied readily or easily to automated decision making.

Gareth Snell (Stoke-on-Trent Central) (Lab/Co-op): My right hon. Friend gives a brilliant example. The point is that employment agencies play an incredibly important role in providing workers for particular sectors of the economy, from hotels to logistics, distribution and construction. The challenge is that the areas of the economy that have created the most jobs in the 10 years since the financial crash are those where terms and conditions are poorest, casualisation is highest and wages are lowest—and they are the areas where productivity is poorest, too. The Government could take a different kind of labour market approach that enhanced productivity and wages, and shut down some of the bad practices and casualisation that are creating a problem.

Liam Byrne: My hon. Friend describes as more virtuous.

I want to give the Committee a couple of examples of why this is so serious, as sometimes a scenario or two can help. Let us take an individual whom we will call “Mr A”. He is a 56-year-old man applying for website development roles. Typically, if someone is applying for jobs in a particular sector, those jobs will be advertised online. In fact, many such roles are advertised only online, and they target users only in the age profile 26 to 35, through digital advertising or social media networks, whether that is Facebook, LinkedIn, or others. Because Mr A is not in the particular age bracket being targeted, he never sees the ad, as it will never pop up on his news feed, or on digital advertising aimed at him. He therefore does not apply for the role and does not know he is being excluded from applying for the role, all as a consequence of him being the wrong age. Since he is excluded from opportunities because of his age, he finds it much harder to find a role.

The Equality Act, which was passed with cross-party consensus, prohibits less favourable treatment because of age—direct discrimination—including in relation to recruitment practices, and protects individuals based on their age. The Act sets out a number of remedies for individuals who have been discriminated against in that way, but it is not clear how the Bill proposes to correct that sin. Injustices in the labour market are multiplying, and there is a cross-party consensus for a stronger defence of workers. In fact, the Member of Parliament for the town where I grew up, the right hon. Member for Harlow (Robert Halfon), has led the argument in favour of the Conservative party rechristening itself the Workers’ party, and the Labour party was founded on a defence of labour rights, so I do not think this is an especially contentious matter. There is cross-party consensus about the need to stand up for workers’ rights, particularly when wages are stagnating so dramatically.

We are therefore not divided on a point of principle, but the Opposition have an ambition to do something about this growing problem. The Bill could be corrected in a way that made a significant difference. There is not an argument about the rights that are already in place, because they are enshrined in the Equality Act, with which Members on both sides of the House have agreed. The challenge is that the law as it stands is deficient and cannot be applied readily or easily to automated decision making.

Liam Byrne: My hon. Friend gives a brilliant example. The point is that employment agencies play an incredibly important role in providing workers for particular sectors of the economy, from hotels to logistics, distribution and construction. The challenge is that the areas of the economy that have created the most jobs in the 10 years since the financial crash are those where terms and conditions are poorest, casualisation is highest and wages are lowest—and they are the areas where productivity is poorest, too. The Government could take a different kind of labour market approach that enhanced productivity and wages, and shut down some of the bad practices and casualisation that are creating a problem.

As it happens, the Government have signed up to some pretty big ambitions in that area. Countries around the world recently signed up to the UN sustainable development goals. Goal 8 commits the Government to reducing inequality, and SDG 10 commits them to reducing regional inequality. However, when I asked the Prime Minister what she was doing about that, my question was referred to Her Majesty’s Treasury and the answer that came back from the Chancellor was, “We believe in raising productivity and growth.” The way to raise productivity and growth is to ensure that
there are good practices in the labour market, because it is poor labour market productivity that is holding us back as a country.

If digital blacklisting or casualisation were to spread throughout the labour market in the sectors that happen to be creating jobs, there would be no increase in productivity and the Government would be embarked on a self-defeating economic policy. Although these new clauses may sound technical, they have a bearing on a much more important plank of the Government’s economic development strategy.

Our arguments are based on principles that have widespread support on both sides of the House and they are economically wise. The consequences of the new clauses will be more than outweighed by the benefits they will deliver. I commend them to the Minister and I hope she will take them on board.

2.15 pm

Darren Jones (Bristol North West) (Lab): I want to add some further comments in support of the new clauses.

The Science and Technology Committee, one of the two Committees that I sit on, has had a detailed debate on algorithmic fairness. It is important to understand what the new clauses seek to do. There is a nervousness about regulating algorithms or making them completely transparent, because there are commercial sensitivities in the coding in respect of the way they are published or otherwise.

These new clauses seek to put the obligation on to the human beings who produce the algorithms to think about things such as equalities law to ensure that we do not hardcode biases into them, as my hon. Friend the Member for Cambridge said on Second Reading. It is important to understand how the new clauses apply to the inputs—what happens in the black box of the algorithm—and the outputs. The inputs to an algorithm are that a human codes and sets its rules, and that they put the data into it for it to make a decision.

The new clauses seek to say that the human must have a consistent and legal obligation to understand the equalities impacts of their coding and data entry into the black box of the algorithm to avoid biases coming out at the other end. As algorithms are increasingly used, that is an important technical distinction to understand, and it is why the new clauses are very sensible. On that basis, I hope the Government will support them.

The Chair: I call the Minister, whose birthday it is today.

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): Thank you, Mr Streeter, and what a wonderful birthday present it is to be serving on the Committee.

It is a joy, actually, to be able to agree with the Opposition on the principle that equality applies not only to decisions made by human beings or with human input, but to decisions made solely by computers and algorithms. On that, we are very much agreed. The reason that we do not support the new clauses is that we believe that the Equality Act already protects workers against direct or indirect discrimination by computer or algorithm-based decisions. As the right hon. Member for Birmingham, Hodge Hill rightly said, the Act was passed with cross-party consensus.

The Act is clear that in all cases, the employer is liable for the outcome of any of their actions, or those of their managers or supervisors, or those that are the result of a computer, algorithm or mechanical process. If, during a recruitment process, applications from people with names that suggest a particular ethnicity were rejected for that reason by an algorithm, the employer would be liable for race discrimination, whether or not they designed the algorithm with that intention in mind.

The right hon. Gentleman placed a great deal of emphasis on advertising and, again, we share his concerns that employers could seek to treat potential employees unfairly and unequally. The Equality and Human Rights Commission publishes guidance for employers to ensure that there is no discriminatory conduct and that fair and open access to employment opportunities is made clear in the way that employers advertise posts.

The same principle applies in the provision of services. An automated process that intentionally or unintentionally denies a service to someone because of a protected characteristic will lay the service provider open to a claim under the Act, subject to any exceptions.

Victoria Atkins: If I may, I will write to the right hon. Gentleman with that precise number, but I know that the Equality and Human Rights Commission is very clear in its guidance that employers must act within the law. The law is very clear that there are to be no direct or indirect forms of discrimination.

The hon. Member for Cambridge raised the GDPR, and talked about looking forwards not backwards. Article 5(1)(a) requires processing of any kind to be fair and transparent. Recital 71 draws a link between ensuring that processing is fair and minimising discriminatory effects. Article 35 of the GDPR requires controllers to undertake data protection impact assessments for all high-risk activities, and article 36 requires a subset of those impact assessments to be sent to the Information Commissioner for consultation prior to the processing taking place. The GDPR also gives data subjects the tools to understand the way in which their data has been processed. Processing must be transparent, details of that processing must be provided to every data subject, whether or not the data was collected directly from them, and data subjects are entitled to a copy of the data held about them.

When automated decision-making is engaged there are yet more safeguards. Controllers must tell the data subject, at the point of collecting the data, whether they intend to make such decisions and, if they do, provide meaningful information about the logic involved, as well as the significance and the envisaged consequences for the data subject of such processing. Once a significant decision has been made, that must be communicated to
the data subject, and they must be given the opportunity to object to that decision so that it is re-taken by a human being.

We would say that the existing equality law and data protection law are remarkably technologically agnostic. Controllers cannot hide behind algorithms, but equally they should not be prevented from making use of them when they can do so in a sensible, fair and productive way.

Daniel Zeichner: Going back to the point raised by my right hon. Friend, I suspect that the number of cases will prove to be relatively low. The logic of what the Minister is saying would suggest that there is no algorithmic unfairness going on out there. I do not think that that is the case. What does she think?

Victoria Atkins: I would be guided by the view of the Equality and Human Rights Commission, which oversees conduct in this area, that it is scaremongering for the Information Commissioner and the Equality and Human Rights Commission are in regular contact. If they are not, I very much hope that this will ensure that they are.

We are clear in law that there cannot be such discrimination as has been discussed. We believe that the framework of the law is there, and that the Information Commissioner’s Office and the Equality and Human Rights Commission, with their respective responsibilities, can help, advise and cajole, and, at times, enforce the law accordingly. I suspect that we will have some interesting times ahead of us with the release of the gender pay gap information. I will do a plug now, and say that any company employing more than 250 employees should abide by the law by 4 April. I look forward to reviewing the evidence from that exercise next month.

We are concerned that new clauses 7 and 8 are already dealt with in law, and that new clauses 9 to 11 would create an entirely new regulatory structure just for computer-assisted decision-making in the workplace, layered on top of the existing requirements of both employment and data protection law. We want the message to be clear to employers that there is no distinction between the types of decision-making. They are responsible for it, whether a human being was involved or not, and they must ensure that their decisions comply with the law.

Having explained our belief that the existing law meets the concerns raised by the right hon. Member for Birmingham, Hodge Hill, I hope he will withdraw the new clause.

Liam Byrne: I think it was in “Candide” that Voltaire introduced us to the word “Panglossian”, and we have heard a rather elegant and Panglossian description of a perfect world in which all is fine in the labour market. I am much more sceptical than the Minister. I do not think the current law is sufficiently sharp, and I am concerned that the consequence of that will be injustice for our constituents.

The Minister raised a line of argument that it is important for us to consider. The ultimate test of whether the law is good enough must be what is actually happening out there in the labour market. I do not think it is good enough; she thinks it is fine. On the nub of the argument, a few more facts might be needed on both sides, so we reserve the right to come back to the issue on Report. This has been a useful debate. I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

New Clause 13

Review of Electronic Commerce (EC Directive) Regulations

“(1) The Secretary of State shall lay before both Houses of Parliament a review of the application and operation of the Electronic Commerce (EC Directive) Regulations 2002 in relation to the processing of personal data.

(2) A review under subsection (1) shall be laid before Parliament by 31 January 2019.”—(Liam Byrne.)

This new clause would order the Secretary of State to review the application and operation of the Electronic Commerce (EC Directive) Regulations 2002 in relation to the processing of personal data.

Brought up, and read the First time.

Liam Byrne: I beg to move, That the clause be read a Second time.

This is not normally my practice, but let me raise another area that is subject to a measure of cross-party consensus. There is widespread recognition that the e-commerce directive, which is used to regulate information services providers, is hopelessly out of date. It was agreed in around 2000. In effect, it allows information services providers to be treated as platforms rather than publishers. Since then, we have seen the growth of big tech and the new data giants that now dominate the digital economy, and they are misbehaving. Worse, they have become platforms for hate speech, social division and interference in democracy. It was intriguing to hear Mark Zuckerberg himself admit in the interview he gave yesterday that Facebook was indeed being used to try to corrupt elections. That is an extraordinary recognition by the head of one of the most important firms in the world.

The Secretary of State for Digital, Culture, Media and Sport reminded us as recently as this morning that as we come out of the European Union we will have a new opportunity to update the e-commerce directive. The House basically must put in place a new framework to regulate information services providers in a new way. A debate is raging among our neighbours about what steps we need to take to shut down the hate speech that is dividing communities, and we need to get into that debate quickly. Germany recently passed laws that require companies such as Facebook to take down hate speech in a very short time window or face fines of up to €10 million and Ireland has created a new regulator to provide a degree of overwatch, so it is intriguing that we are falling behind some of our most important neighbours, who now lead this debate.

I began looking at this issue when I started researching new techniques in ISIS propaganda. In the excellent Scotland Yard counter-terrorism referral unit, I saw propaganda that was put together with the slickness of a pop video to incite people to commit the most heinous crimes, such as the one we commemorate today. Yet I think we all recognise that organisations such as Facebook and YouTube are simply not working quickly enough to take down that kind of material, which we simply do...
not want people to see. I congratulate *The Times*, which has run a forensic campaign to shine a light on some of that bad practice. It is good finally to see advertisers such as Unilever beginning to deliver a tougher message to social media platforms that enough is enough.

We know we have to modernise those regulations. The commercial world and politicians on both sides are saying, “Enough is enough.” We all fear the consequences of things going wrong with respect to the destabilisation of democracy in America—but not just in America. We have seen it across the Baltics, in France, in Germany, across southern Europe and in eastern Europe. Among our NATO allies, we can see a vulnerability to our enemies using social media platforms to sow division.

The new clause urges the Government to get on with the Government to put some deeds behind those grand words. We can sit on our hands or do something about it. I suggest we do something about it.

The new clause would set a deadline for Government proposals to modernise the e-commerce directive. We will have to have a debate and make a choice about how close we bring the obligations and the liabilities of social media firms to the regulations we have for newspapers. Despite the hopelessly weak regulatory regime that the Government are intent on delivering in this country, there is no way on earth that even an IPSO-regulated newspaper could get away with the kind of nonsense that we see on social media—the kind of hate speech and viciousness that, more often than not I might add, is directed at women rather than men.

The new clause urges the Government to get on with that and states that by 31 January 2019—a little under a year’s time—we would have not the final law or regulations, but a review and a set of proposals on how the e-commerce directive needed to be reformed.

To my friends in the technology industry—as a former technology entrepreneur, I have many—I often make the point that we did not have one factory Act during the 19th century; we had 17. As technology, the economy, and custom and practice in the workplace changed, we had to update and modernise the regulation in this country. Frankly, that is the journey we are now on.

The Secretary of State vividly and colourfully said in *The Times*, and in his podcast with Nick Robinson, which comes out tomorrow, that the wild west is over and a new order will descend. The new clause urges the Government to put some deeds behind those grand words.

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): I agree with everything the right hon. Gentleman has said, except that I do not think the Bill is the place for his proposals. The e-commerce directive and the Electronic Commerce (EC Directive) Regulations 2002, which transpose it into UK law, regulate services that are “normally provided for remuneration, at a distance, by means of electronic equipment…and at the individual request of a recipient of a service”.

Those services are known as information society services.

However, questions relating to the processing of personal data by information society services are excluded from the scope of the e-commerce directive and hence excluded from the scope of the 2002 regulations. That is because the processing of personal data is regulated by other instruments, including, from May, the GDPR. The review of the application and operation of the 2002 regulations solely in relation to the processing of personal data, as proposed by new clause 13, would therefore be a speedy review to undertake.

However, that does not address the substance of the right hon. Gentleman’s concern, which we have already discussed in a delegated legislation Committee earlier this month. As I said then, the Government are aware of his concern that the e-commerce directive, finalised in 2000, is now outdated, in particular with regard to its liability provisions.

Those provisions limit, in specified circumstances, the liability that service providers have for the content on their sites. That includes social media platforms where they act as hosts. Social media companies have made limited progress on a voluntary basis, removing some particularly harmful content quickly and, in recent years, consistently. However, as we have seen in the case of National Action and its abhorrent YouTube videos, and many other lower-profile cases, there is a long way to go. We do not rule out legislation.

The Government have made it clear through our digital charter that we are committed to making the UK the safest place to be online, as well as the best place to grow a digital business. As the Prime Minister has said, when we leave the EU we will be leaving the digital single market, including the e-commerce directive. That gives us an opportunity to make sure that we get matters corrected for the modern age: supporting innovation and growth, and the use of modern technology, but doing so in a way that commands the confidence of citizens, protects their rights and makes their rights as enforceable online as they currently are offline.

The UK will be leaving the digital single market, but we will continue to work closely with the EU on digital issues as we build up our existing strong relationship in the future economic partnership. We will work closely with a variety of partners in Europe and further afield. Alongside that, our internet safety strategy will tackle the removal of harmful but legal content. Through the introduction of a social media code of practice and annual transparency report, we will place companies under an obligation to respond quickly to user reports and to ensure that their moderation processes are fit for purpose, with statutory backing if required. We have demonstrated that in the example of the introduction of age verification for online pornography.

There is an important debate to be had on the e-commerce directive and on platform liability, and we are committed to working with others, including other countries, to understand how we can make the best of existing frameworks and definitions. Consideration of the Bill in Committee and Report are not the right places for that wide debate to be had. For those reasons, I request that the right hon. Gentleman withdraw the clause.
Liam Byrne: I admire the Minister’s concern and ambition for administrative tidiness. She reminds me of an old quote by Bevin, who said once, “If you are a purist, the place for you is not a Parliament; it is a monastery.”

Margot James: A nunnery.

Liam Byrne: In the case of the Minister, a nunnery, although Bevin was less enlightened than the hon. Lady. Here is a Bill; here is a new clause; the new clause is within scope. The object of the new clause is to deliver a Government objective, yet it is rejected. That is hard logic to follow. We have had the tremendous assurance, however, that there will be nothing less than a code of practice, so these huge data giants will be shaking in their boots in California, when they wake up. They will be genuinely concerned and no doubt already planning how they can reform their ways and stop the malpractice that we have grown all too used to. I am afraid that these amount to a collection of warm words, when what the country needs is action. With that in mind, I will push the new clause to a vote.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 7, Noes 10.

Division No. 15]

AYES

Byrne, rh Liam
Elmore, Chris
Jones, Darren
McDonald, Stuart C.

NOES

Adams, Nigel
Atkins, Victoria
Clark, Colin
Heaton-Jones, Peter
Huddleston, Nigel

Question accordingly negatived.

New Clause 16

CODE ON PROCESSING PERSONAL DATA IN EDUCATION

“(1) The Commissioner must consult on, prepare and publish a code of practice on standards to be followed in relation to the collection, processing, publication and other dissemination of personal data concerning children and pupils in connection with the provision of education services, which relates to the rights of data subjects, appropriate to their capacity and stage of education.

(2) Before preparing a code or amendments under this section the Commissioner must consult the Secretary of State and such other persons as the Commissioner considers appropriate as set out in Clause 124 (3).

(3) In preparing a code or amendments under this section, the Commissioner must have regard—

(a) that children have different capacity independent of age, including pupils who may be in provision up to the age of 25; and


(4) For the purposes of subsection (1), “the rights of data subjects” must include—

(a) measures related to Articles 24(1) (responsibility of the controller), 25 (data protection by design and by default) and 32(3) (security of processing) of the GDPR;

(b) safeguards and suitable measures with regard to Articles 22(2)(b) (automated individual decision-making, including profiling), Recital 71 (data subject rights on profiling as regard a child) and 23 (restrictions) of the GDPR;

(c) the rights of data subjects to object to or restrict the processing of their personal data collected during their education, under Articles 8 (child’s consent to Information Society Services), 21 (right to object to automated individual decision making, including profiling) and 18(2) (right to restriction of processing) of the GDPR;

(d) where personal data are biometric or special categories of personal data as described in Article 9(1) of the GDPR, the code should set out obligations on the controller and processor to register processing of this category of data with the Commissioner where it concerns a child, or pupil in education; and

(e) matters related to the understanding and exercising of rights relating to personal data and the provision of education services.”—(Liam Byrne.)

This new clause would require the Information Commissioner to consult on, prepare and publish a code of practice on standards to be followed in relation to the collection, processing, publication and other dissemination of personal data concerning children and pupils in connection with the provision of education services.

Brought up, and read the First time.

Liam Byrne: I beg to move, That the clause be read a Second time.

This is another entirely sensible new clause, which I hope the Government will take on board, either at this stage or on Report. We rehearsed earlier in Committee the debate about the reality and challenges of the fact that our education providers are now collecting, managing and often losing significant amounts of very personal data relating to children.

Any of us who has children at school will know the joys of ParentPay, which means that schools are collecting biometric data on our children. We know that schools are keeping exam results and all kinds of records and evaluations about our children online. Given the complexity of the GDPR and some of the costs and questions around implementing it, the complexity of the education system means that we urgently need a code of practice that schools can draw on to help them get the GDPR right, and to help our educators in their task of keeping our children’s data safer than it is today.

In my argument, I will draw on the excellent contribution made on Second Reading by my noble Friend, Lord Knight, who said:

“Schools routinely use commercial apps for things such as recording behaviour, profiling children, cashless payments, reporting” and so on. My noble Friend has long been an advocate of that kind of thing, but the point is that he knows, and the other place recognised, that the way school information systems operate means they are often cloud based and integrated into all sorts of other data systems. There will often be contracts in place with all sorts of education service providers, which will entail the transfer of data between, for example, a school and a third party. It could well be that that third party is based overseas. As my noble Friend said:
“Schools desperately need advice on GDPR compliance to allow them to comply with this Bill when it becomes law.”—[Official Report, House of Lords, 10 October 2017; Vol. 785, c. 185.]

Lord Storey rode in behind my noble Friend, saying that “young people probably need more protection than at any other time in our recent history.”—[Official Report, House of Lords, 10 October 2017; Vol. 785, c. 170.]

That is not something that has been debated only by the other place. UNICEF recently published a working paper entitled “Privacy, protection of personal information and reputation rights” and said it was now “evident that children’s privacy differs both in scope and application from adults’ privacy” but that they experience more threats than any other group. The “Council of Europe Strategy for the Rights of the Child (2016-2021)” echoed the same sentiment and observed:

“Parents and teachers struggle to keep up with technological developments”.

I have a number of friends who are teachers and headteachers. They listen to me in horror when I explain that I am the shadow Minister for the Data Protection Bill, because they know this is looming and they are absolutely terrified of it. Why is that? Because they are good people and good educators; they go into teaching because they want to change the world and change children’s lives, and they recognise the new obligations that are coming, but they also recognise the realities of how their schools operate today. Those people know about the proliferation of data that they and their staff are collecting. They know about the dangers and risks of that data leaking—not least because most teachers I know who have some kind of pastoral care responsibility seem to spend half their time having to advise their children about what not to do with social media apps and what not to post. They are often drawn in to disputes that rage out of control on social media platforms such as Instagram.

Teachers are very alert to the dangers of this new world. They are doing a brilliant and innovative job of supporting children through it, but they are crying out now for good guidance to help them to implement the GDPR successfully.

2.45 pm

Gareth Snell: I echo my right hon. Friend’s points. My daughter is seven years old. I have an app on my phone that, at any time of the day, will tell me what she is doing at school. Her attendance, reward system, and school meal requirements are all recorded on it, and I can access it at any time. The school she goes to wants them to do their job of improving children’s education. However, it has costs and consequences too. I hope that Her Majesty’s Government will look sympathetically on the task of teachers, as they confront this 200-and-heaven-knows-what-page Bill.

Darren Jones (Bristol North West) (Lab): Does my right hon. Friend share my concerns that, in response to a number of written parliamentary questions that I tabled, it became clear that the Government gave access to the national pupil database, which is controlled by the Government, to commercial entities, including newspapers such as The Daily Telegraph?

Liam Byrne: Yes. My hon. Friend has done an extraordinary job of exposing that minor scandal. I am surprised that it has not had more attention in the House, but hopefully once the Bill has passed it is exactly the kind of behaviour that we can begin to police rather more effectively.

I am sure that Ministers will recognise that there is a need for this. No doubt their colleagues in the Department for Education are absolutely all over it. I was talking to a headteacher in the Minister’s own constituency recently—an excellent headteacher, in an excellent school, who is a personal friend. The horror with which headteachers regard the arrival of the GDPR is something to behold. Heaven knows, our school leaders and our teachers have enough to do. I call on Ministers to make their task, their lives, and their mission that bit easier by accepting the new clause.

Victoria Atkins: Our schools handle large volumes of sensitive data about the children they educate. Anyone who has any involvement with the education system, either personally through their families, on their mobile phone apps, or in a professional capacity as constituency MPs, is very conscious of the huge responsibilities that school leaders have in handling that data properly and well, and in accordance with the law. As data controllers in their own right, schools and other organisations in the education system will need to ensure that they have adequate data-handling policies in place to comply with their legal obligations under the new law.

Work is going on already. The Department for Education has a programme of advice and education for school-leaders, which covers everything from blogs, a guidance video, speaking engagements, and work to encourage system suppliers to be proactive in helping schools to become GDPR-compliant. Research is also being undertaken with parents about model privacy notices that will help schools to make parents and pupils more aware of the data about children used in the sector. The Department for Education is also shaping a toolkit that will bring together various pieces of guidance and best practice to address the specific needs of those who process education data. In parallel, the Information Commissioner has consulted on guidance specifically addressing issues about the fair and lawful processing of children’s data. Everyone is very alive to the issue of protecting children and their data.

At this point, the Government want to support the work that is ongoing—already taking place—and the provisions on guidance that are already in the Bill. Our
concern is that legislating for a code now could be seen as a reason for schools to wait and see, rather than continuing their preparations for the new law. But it may be that in due course the weight of argument swings in favour of a sector-specific code of practice. That can happen. It does not have to be in the Bill. It can happen because clause 128 provides that the Secretary of State may require the Information Commissioner to prepare additional codes of practice for the processing of personal data, and the commissioner can issue further guidance under her own steam, using her powers under article 57 of the GDPR, without needing any direction from the Secretary of State.

I hope that the ongoing work reassures the right hon. Gentleman and that he will withdraw the new clause at this stage.

Liam Byrne: I am reassured by that and I beg to ask leave to withdraw the motion.
Clause, by leave, withdrawn.

New Clause 17
PERSONAL DATA ETHICS ADVISORY BOARD AND ETHICS CODE OF PRACTICE

'(1) The Secretary of State must appoint an independent Personal Data Ethics Advisory Board ("the board").

(2) The board's functions, in relation to the processing of personal data to which the GDPR and this Act applies, are—
(a) to monitor further technical advances in the use and management of personal data and their implications for the rights of data subjects;
(b) to monitor the protection of the individual and collective rights and interests of data subjects in relation to their personal data;
(c) to ensure that trade-offs between the rights of data subjects and the use of management of personal data are made transparently, inclusively, and with accountability;
(d) to seek out good practices and learn from successes and failures in the use and management of personal data;
(e) to enhance the skills of data subjects and controllers in the use and management of personal data.

(3) The board must work with the Commissioner to prepare a data ethics code of practice for data controllers, which must—
(a) include a duty of care on the data controller and the processor to the data subject;
(b) provide best practice for data controllers and processors on measures, which in relation to the processing of personal data—
(i) reduce vulnerabilities and inequalities;
(ii) protect human rights;
(iii) increase the security of personal data; and
(iv) ensure that the access, use and sharing of personal data is transparent, and the purposes of personal data processing are communicated clearly and accessibly to data subjects.

(4) The code must also include guidance in relation to the processing of personal data in the public interest and the substantial public interest.

(5) Where a data controller or processor does not follow the code under this section, the data controller or processor is subject to a fine to be determined by the Commissioner.

(6) The board must report annually to the Secretary of State.

(7) The report in subsection (6) may contain recommendations to the Secretary of State and the Commissioner relating to how they can improve the processing of personal data and the protection of data subjects' rights by improving methods of—
(a) monitoring and evaluating the use and management of personal data;
(b) sharing best practice and setting standards for data controllers; and
(c) clarifying and enforcing data protection rules.

(8) The Secretary of State must lay the report made under subsection (6) before both Houses of Parliament.

(9) The Secretary of State must, no later than one year after the day on which this Act receives Royal Assent, lay before both Houses of Parliament draft regulations in relation to the functions of the Personal Data Ethics Advisory Board as listed in subsections (2), (3), (4), (6) and (7) of this section.

(10) Regulations under this section are subject to the affirmative resolution procedure. —(Darren Jones.)

This new clause would establish a statutory basis for a Data Ethics Advisory Board.

Brought up, and read the First time.

Darren Jones: I beg to move, That the clause be read a Second time.

New clause 17 is in my name and that of my right hon. Friend the Member for Birmingham, Hodge Hill. I do not take it personally that my other hon. Friends have not signed up to it; that was probably my fault for not asking them to do so in advance.

The new clause would bring a statutory footing to the data and artificial intelligence ethics unit, which I am very pleased that the Government have now funded and established, through the spring statement, in the Minister's Department. It comes off the back of conversations with the Information Commissioner in Select Committee about the differing roles of enforcing legislation and having a public debate about what is right and wrong and what the boundaries are in this ever-changing space. The commissioner was very clear that we need to have that debate with the public, but that it is not for her to do it. The ICO is an enforcer of legislation. The commissioner has a lot on her plate and is challenged by her own resource as it is. She felt that the new unit in the Department would be a good place to have the debate about technology ethics, and I support that assertion.

With no disrespect to any colleagues, I do not think that the House of Commons, and perhaps even the Select Committees to a certain extent, necessarily has the time, energy or resource to get into the real detail of some of the technology ethics questions, nor to take them out to the public, who are the people we need to be having the debate with.

The new clause would therefore establish in law that monitoring, understanding and public debate obligation that I, the ICO and others agree ought to exist in the new data ethics unit, but make it clear that enforcement was reserved for the Information Commissioner. I tabled the new clause because, although I welcome the Government's commitment to the data and AI ethics unit, I feel that there is potential for drift. The new clause would therefore put an anchor in the technology ethics requirement of the unit so that it understands and communicates the ethical issues and does not necessarily get sidetracked into other issues, although it may seek to do that on top of this anchor. However, I think this anchor needs to be placed.

Also, I recognise that the Minister and the Secretary of State supported the recommendation made previously under the Cameron Government and I welcome that,
but of course, with an advisory group within the Department, it may be a future Minister’s whim that they no longer wish to be advised on these issues, or it may be the whim of the Treasury—with, potentially, budget cuts—that it no longer wishes to fund the people doing the work. I think that that is not good enough and that putting this provision in the Bill would give some security to the unit for the future.

I will refer to some of the comments made about the centre for data ethics and innovation, which I have been calling the data and AI ethics unit. When it was first discussed, in the autumn Budget of November 2017, the Chancellor of the Exchequer said that the unit and that putting this provision in the Bill would give some security to the unit for the future.

I move on to some of the documents from the recruitment advertising for personnel to run the unit from January of this year, which said that the centre will be at the centre of plans to make the UK the best place in the world for AI businesses. Again, that is a positive statement, but one about AI business adoption in this country, not ethical requirements. It also said that the centre would advise on ethical and innovative uses of data-driven tech. Again, that is a positive statement, but I just do not think it is quite at the heart of understanding and communicating the ethical challenges that we need to try to understand and legislate for.

My concern is that while all this stuff is very positive, and I agree with the Government that we need to maintain our position as a world leader in artificial intelligence and that it is something we need to be very proud of—especially as we go through the regrettable process of leaving the European Union and the single market, we need to hold on to the strengths we have in the British economy—this week has shown that there is a need for an informed public debate on ethics. As no doubt all members of the Committee have read in my New Statesman article of today, one of the issues we have as the voice of our constituents in Parliament is that in order for our constituents to understand or take a view on what is right or wrong in this quickly developing space, we all need to understand it in the first place—to understand what is happening with our data and in the technology space, to understand what is being done with it and, having understood it, to then to take a view about it. The Cambridge Analytica scandal has been so newsworthy because the majority of people understandably had no idea that all this stuff was happening with their data. How we legislate for and set ethical frameworks must first come from a position of understanding.

That is why the new clause sets out that there should be an independent advisory board. The use of such boards is commonplace across Departments and I hope that would not be a contentious question. Subsection (2) talks about some of the things that that board should do. The Minister will note that the language I have used is quite careful in looking at how the board should monitor developments, monitor the protection of rights and look out for good practice. It does not seek to step on the toes of the Information Commissioner or the powers of the Government, but merely to understand, educate and inform.

The new clause goes on to suggest that the new board would work with the commissioner to put together a code of practice for data controllers. A code of practice with a technology ethics basis is important because it says to every data controller, regardless of what they do or what type of work they do, that we require ethical boundaries to be set and understood in the culture of what we do with big data analytics in this country. In working with the commissioner, this board would add great value to the way that we work with people’s personal data, by setting out that code of practice.

I hope that the new clause adds value to the work that the Minister’s Department is already doing. My hope is that by adding it to the Bill—albeit that current Parliaments cannot of course bind their successors and it could be legislated away in the future—it gives a solid grounding to the concept that we take technology ethical issues seriously, that we seek to understand them properly, not as politicians or as busy civil servants, but as experts who can be out with our stakeholders understanding the public policy consequences, and that we seek to have a proper debate with the public, working with enforcers such as the ICO to set, in this wild west, the boundaries of what is and is not acceptable. I commend the new clause to the Committee and hope that the Government will support it.

Margot James: I thank the hon. Gentleman for raising this very important subject. He is absolutely right. Data analytics have the potential to transform whole sectors of society and the economy—law enforcement and healthcare to name but some. I agree with him that a public debate around the issues is required, and that is one of the reasons why the Government are creating the centre for data ethics and innovation, which he mentioned. The centre will advise the Government and regulators on how they can strengthen and improve the way that data and AI are governed, as well as supporting the innovative and ethical use of that data.

3 pm

The centre will look at issues relating to both personal and non-personal data. Lord Stevenson of Balmacara said in the other place that “it has not been possible to find a form of words for the powers that would be used to set up this advisory board”—the board is mentioned in the new clause—“which would be sufficiently broad to give a proper basis for the ambitions that we all share for it.”—[Official Report, House of Lords, 10 January 2018; Vol. 788, c. 297.] I feel that the new clause brings us back to the point that Lord Stevenson said was problematic.

We plan to consult on the centre in the summer, after the chair has been appointed; we anticipate that appointment will be made in May. We would very much welcome the input of the hon. Member for Bristol North West, who is very knowledgeable on this issue.

The new clause would extend the commissioner’s remit far beyond the application of what is required of her as the UK’s supervisory authority for data protection. Given the breadth of the code that is set out in the new clause, it would essentially require the commissioner to...
become a regulator on a much more significant scale than at present, and it would also create an overlap with the Electoral Commission, which is a separate regulator.

Three is more here that we agree on than disagree on, but the centre for data ethics and innovation, which we are in the process of creating, will, I trust, be the answer to much of the issue raised by the hon. Gentleman in his new clause. I hope that he feels confident enough in that to withdraw it.

Darren Jones: I thank the Minister for her co-operative words and for the invitation to be part of this developing area of public policy. Having already plugged my *New Statesman* article, I will plug a part of it, which is the news that, having worked with some of the all-party parliamentary groups, I am pleased that we will launch a commission on technology ethics with one of the Minister’s colleagues, whose constituency I cannot quite remember, I am afraid, so I cannot make reference to him. But he is excellent.

We look forward to working with industry, stakeholders and politicians on a cross-party basis, to get into the debate about technology ethics. I accept the Minister’s warm words about co-operating on this issue positively, so that hopefully the outcomes of this commission can perhaps help to influence the work of the unit, or centre, and the Government’s response to it.

I would like this new unit to be given a statutory basis, to show its importance. It is vital that it has clout across Government and across Departments, so that it is not just a positive thing when we have Ministers who are willing to take part in and listen to this debate and instead is something that will go on with successive Ministers, should the current Minister be promoted, and with future Governments, too. However, in return for the Minister’s warm words of co-operation, I am happy not to press the new clause to a vote today.

Daniel Zeichner: Very briefly, I declare an interest as the chair of the all-party parliamentary group on data analytics. This is a subject, of course, that is very dear to our hearts. I will just say that there is a great deal of common ground on it. I commend my hon. Friend the Member for Bristol North West for trying to put it into the Bill, because I, too, think it needs to be put on a statutory basis. However, I will just draw attention to a lot of the very good work that has been done by a whole range of people in bringing forward the new structures.

I will just say again that in general I think we are heaping a huge amount of responsibility on the Information Commissioner; frankly, we are now almost inviting her to save the world. She and her office will need help. So an additional body, with resources, is required.

The Royal Society and the British Academy have done a lot of work on this issue over the last few years. I will conclude by referring back to a comment made by the hon. Member for Gordon, because it is worth saying that the Royal Society and the British Academy state in the conclusions of their report:

“It is essential to have a framework that engenders trust and confidence, to give entrepreneurs and decision-makers the confidence to act now, and to realise the potential of new applications in a way that reflects societal preferences.”

That is exactly the kind of thing we are trying to achieve. This body is essential and it needs to be set up as quickly as possible.

Darren Jones: I beg to ask leave to withdraw the new clause.

Clause, by leave, withdrawn.

New Clause 20

**Automated number plate recognition (No. 2)**

“(1) Vehicle registration marks captured by automated number plate recognition systems are personal data.

(2) The Secretary of State shall issue a code of practice in connection with the operation by the police of automated number plate recognition systems.

(3) Any code of practice under subsection (1) shall conform to section 67 of the Police and Criminal Evidence Act 1984.”

(Liam Byrne.)

This new clause requires the Secretary of State to issue a code of practice in connection with the operation by the police of automated number plate recognition systems, vehicle registration marks captured by which are to be considered personal data in line with the opinion of the Information Commissioner.

Brought up, and read the First time.

Liam Byrne: I beg to move, That the clause be read a Second time.

I will touch on this new clause only very briefly, because I hope the Minister will put my mind at rest with a simple answer. For some time, there has been concern that the way in which data collected by the police through automatic number plate recognition technology is not adequately ordered, organised or policed by a code of practice. A code of practice is probably required to put the police well and truly within the boundaries of the Police and Criminal Evidence Act 1984, the Data Protection Act 1998 and the Bill.

With this new clause, we are basically asking the Secretary of State to issue a code of practice in connection with the operation by the police of ANPR systems under subsection (1), and we ask that it conform to section 67 of the Police and Criminal Evidence Act 1984. I hope the Minister will just say that a code of practice is on the way so we can safely withdraw the new clause.

Victoria Atkins: I hope Committee members have had the chance to see my response to the questions of the hon. Member for Sheffield, Heeley on Tuesday about ANPR, other aspects of surveillance and other types of law enforcement activity.

I assure the right hon. Member for Birmingham, Hodge Hill that ANPR data is personal data and is therefore caught by the provisions of the GDPR and the Bill. We recognise the need to ensure the use of ANPR is properly regulated. Indeed, ANPR systems are governed by not one but two existing codes of practice. The first is the code issued by the Information Commissioner, exercising her powers under section 51 of the Data Protection Act 1998. It is entitled “In the picture: A data protection code of practice for surveillance cameras and personal information”, and was published in June 2017. It is clear that it covers ANPR. It also refers to data protection impact assessments, which we debated last week. It clearly states that where the police and others use or intend to use an ANPR system, it is important that they
“undertake a privacy impact assessment to justify its use and show that its introduction is proportionate and necessary.”

The second code is brought under section 29 of the Protection of Freedoms Act 2012, which required the Secretary of State to issue a code of practice containing guidance about surveillance camera systems. The “Surveillance camera code of practice”, published in June 2013, already covers the use of ANPR systems by the police and others. It sets out 12 guiding principles for system operators. Privacy is very much a part of that. The Protection of Freedoms Act established the office of the Surveillance Camera Commissioner, who has a number of statutory functions in relation to the code, including keeping its operation under review.

In addition, a published memorandum of understanding between the Surveillance Camera Commissioner and the Information Commissioner sets out how they will work together. We also have the general public law principles of the Human Rights Act 1998 and the European convention on human rights. I hope that the two codes I have outlined, the Protection of Freedoms Act and the Human Rights Act reassure the right hon. Gentleman, and that he will withdraw his new clause.

Liam Byrne: I am indeed mollified. I beg to ask leave to withdraw the clause.

Clause, by leave, withdrawn.

New Clause 21

TARGETED DISSEMINATION DISCLOSURE NOTICE FOR THIRD PARTIES AND OTHERS (NO. 2)

"In Schedule 19B of the Political Parties, Elections and Referendums Act 2000 (Power to require disclosure), after paragraph 10 (documents in electronic form) insert—

10A (1) This paragraph applies to the following organisations and individuals—

(a) a recognised third party (within the meaning of Part 6);
(b) a permitted participant (within the meaning of Part 7);
(c) a regulated donee (within the meaning of Schedule 7);
(d) a regulated participant (within the meaning of Schedule 7A);
(e) a candidate at an election (other than a local government election in Scotland);
(f) the election agent for such a candidate;
(g) an organisation or a person notified under subsection 2 of this section;
(h) an organisation or individual formerly falling within any of paragraphs (a) to (g); or
(i) the treasurer, director, or another officer of an organisation to which this paragraph applies, or has been at any time in the period of five years ending with the day on which the notice is given.

(2) The Commission may under this paragraph issue at any time a targeted dissemination disclosure notice, requiring disclosure of any settings used to disseminate material which it believes were intended to have the effect, or were likely to have the effect, of influencing public opinion in any part of the United Kingdom, ahead of a specific election or referendum, where the platform for dissemination allows for targeting based on demographic or other information about individuals, including information gathered by information society services.

(3) This power shall not be available in respect of registered parties or their officers, save where they separately and independently fall into one or more of categories (a) to (i) of sub-paragraph (1).

(4) A person or organisation to whom such a targeted dissemination disclosure notice is given shall comply with it within such time as is specified in the notice."

This new clause would amend the Political Parties, Elections and Referendums Act 2000 to allow the Electoral Commission to require disclosure of settings used to disseminate material where the platform for dissemination allows for targeting based on demographic or other information about individuals.—[Liam Byrne]

Brought up, and read the First time.

Liam Byrne: I beg to move, That the clause be read a Second time.

The Chair: With this it will be convenient to discuss new clause 22—"Election material: personal data gathered by information society services—"

“In section 143 of the Political Parties, Elections and Referendums Act 2000 (Details to appear on electoral material), leave out subsection (1)(b) and insert—

(b) in the case of any other material, including material disseminated through the use of personal data gathered by information society services, any requirements falling to be complied with in relation to the material by virtue of regulations under subsection (6) are complied with."

This new clause would amend the Political Parties, Elections and Referendums Act 2000 to ensure that "any other material" clearly can be read to include election material disseminated through the use of personal data gathered by information society services.

Liam Byrne: I am happy to end on a note of cross-party consensus. We agree that we need to modernise our hopelessly outdated election laws. The news a couple of hours ago that the Information Commissioner’s application for a search warrant at Cambridge Analytica has been deferred—suspended until tomorrow—underlines the fact that the laws we have today for investigating malpractice that may impinge on the health of our democracy are hopelessly inadequate. The Information Commissioner declared to the world—for some reason on live television on Monday—that she was seeking a warrant to get into Cambridge Analytica’s office. Five days later there is still no search warrant issued by a court. Indeed, the court has adjourned the case until tomorrow.

I suspect that Cambridge Analytica has now had quite enough notice to do whatever it likes to the evidence that the Information Commissioner sought. This basket of clauses seeks to insert common-sense provisions to update the law in a way that will ensure that the data protection regime we put in place safeguards the health and wellbeing of our democracy. We need those because of what we now know about allegedly bad companies such as Cambridge Analytica, and because of what we absolutely know about bad countries such as Russia. We have been slow to wake up to the reality that, since 2012, Russia has been operating a new generation of active measures that seek to divide and rule its enemies.

There is no legal definition of hybrid war, so there is no concept of just war when it comes to hybrid war. There is no Geneva convention for hybrid war that defines what is good and what is bad and what is legal and illegal, but most legal scholars agree that a definition
of hybrid war basically touches on a form of intervening against enemies in a way that is deniable and sometimes not traceable. It contains a basket of measures and includes the kind of tactics that we saw deployed in Crimea and Ukraine, which were of course perfected after the invasion of Georgia. We see it in the Baltics and now we see it not just in America but across western Europe as well.

Such a technique—a kind of warcraft of active measures—has a very long history in Russia. Major-General Kalugin, the KGB’s highest ranking defector, once described the approach as the “heart and soul” of Soviet intelligence. The challenge today is that that philosophy was comprehensively updated by General Gerasimov, the Russian Army’s chief of staff, and it came alongside a very different world view presented by President Putin after his re-election as President in 2012 and in his first state of the union address in 2013. It was in that address that President Putin attacked what he called a de-Christianised morally ambivalent west. He set out pretty categorically a foreign policy of contention rather than co-operation.

Since 2012, we have seen what is basically a history of tactical opportunism. A little bit unlike the Soviet era, what we now have are sometimes authorised groups, sometimes rogue groups, seeking openings where they can and putting in place disruptive measures. They are most dangerous when they target the messiness of digital democracy. Here we have a kind of perfection of what I have called in the past a dark social playbook—for example, hackers such as Cozy Bear or Fancy Bear attacked the Democratic National Committee during the American elections.

We also have a partnership with useful idiots such as WikiLeaks, an unholy alliance with what are politely called fake news sites such as Westbrook or indeed Russia Today or Breitbart, which spread hatred. We have a spillover into Twitter. Once a row is brewing on Twitter, we get troll farms such as the Internet Research Agency in St Petersburg kicking in. Half of the tweets about NATO in the Baltics are delivered by robo-trolls out of Russia. It is on an absolutely enormous scale. Once the row is cooking on Twitter, we get the import into Facebook groups. They are private groups and dark groups, and it is perfectly possible to switch on dark money behind those ads circulating the hate material to thousands and thousands if not millions.

We know that that was standard practice in the German and French elections. There is a risk—we do not know what the risk is because the Government will not launch an inquiry—that such activity was going on in the Brexit campaign. I anticipate that there will be more revelations about that this weekend. However, the challenge is that our election law is now hopelessly out of date.

3.15 pm

There is a ban on political advertising on television, which is well established under section 321(2) of the Communications Act 2003. However, although political advertising is banned on television, psychographically targeted ads on Facebook are perfectly legal. In fact, the Advertising Standards Authority has resiled from setting itself up as a truth commission that regulates political advertising, does not patrol or regulate political advertising on television. That is not an issue because there is no political advertising any on television, but there is a lot of it on social media platforms, where it basically goes unregulated.

In addition, we have no provisions to shut down material against hate speech, because the e-commerce directive is so out of date. The Electoral Commission has no power to pursue the foreign money coming in behind some of these dark social ads. When I pressed it on that, it was clear that it does not have the power to pursue things abroad. Ofcom, too, does not regulate the content of video on social media platforms. We therefore have a situation where none of the Electoral Commission, Ofcom and the ASA has the power needed to operate, police and regulate political advertising and political campaigns in the digital era. We learn today that the Information Commissioner does not even have the power to get a search warrant when she needs one to investigate bad behaviour when compelling evidence comes to light.

It is clear that the law is hopelessly outdated. I hope this is a subject on which we can agree. We are now at the receiving end of a new generation of active measures, which are one of the greatest threats to us since the emergence of al-Qaeda at the beginning of the century. We must redouble our defences, so the new clause would give the Electoral Commission the power to issue targeted disclosure notices that require those who seek to influence a political campaign to share with the world information about who is being targeted with what and—crucially—who is writing the cheques.

Margot James: I will be brief in answering some of the serious matters raised by the right hon. Gentleman. The Information Commissioner, as the data regulator, is investigating alleged abuses as part of a broader investigation into the use of personal data during political campaigns. I have said many times that the Bill will add significantly to the commissioner’s powers to conduct investigations, and I have confirmed that we keep an open mind and are considering actively whether further powers are needed in addition to those set out in the Bill.

The Electoral Commission is the regulator of political funding and spending. The commission seeks to bring transparency to our electoral system by enforcing rules on who can fund and how money can be spent, but new clause 21 is about sending the commission into a whole new field: that of personal data regulation. That field is rightly occupied by the Information Commissioner. We can debate whether she needs more powers in the light of the current situation at Cambridge Analytica, and as I have said we are reviewing the Bill.

While the Electoral Commission already has the power to require the disclosure of documents in relation to investigations under its current remit, new clause 21 would provide the commission with new powers to require the disclosure of the settings used to disseminate material. However, understanding how personal data is processed is outside the commission’s remit.

The right hon. Gentleman suggested that his amendment would help with transparency on who is seeking to influence elections, which is very much needed in the current climate. The Government take the security and integrity of democratic processes very seriously. It is absolutely unacceptable for any third country to interfere in our democratic elections or referendums.
On new clause 22, the rules on imprints in the Political Parties, Elections and Referendums Act 2000 are clear. The current rules apply to printed election material no matter how it is targeted. However, the Secretary of State has the power under section 143 to make regulations covering imprints on other types of material, including online material. New clause 22 would therefore not extend the type of online material covered by such regulations. We therefore believe the new clause is unnecessary. The law already includes printed election material disseminated through the use of personal data gathered by whatever means, and the Government will provide further clarity on extending those rules to online material in due course by consulting on making regulations under the power in section 143(6).

On that basis, I ask the right hon. Gentleman to withdraw his new clause.

Liam Byrne: That is a deeply disappointing answer. I was under the impression that the Secretary of State said in interviews today that he is open-minded about the UK version of the Honest Ads Act that we propose. That appears to be in some contrast to the answer that the Minister offered.

What this country has today is an Advertising Standards Authority that does not regulate political advertising; Ofcom, which does not regulate video when it is online; an Electoral Commission without the power to investigate digital campaigning; and an Information Commissioner who cannot get a search warrant. Worse, we have a Financial Conduct Authority that, because it does not have a data sharing gateway with the Electoral Commission, cannot share information about the financial background of companies that might have been laundering money going into political and referendum campaigns. The law is hopelessly inadequate. Through that great hole, our enemies are driving a coach and horses, which is having a huge impact on the health and wellbeing of our democracy.

That is not a day-to-day concern in Labour constituencies, but it is for the Conservative party. Voter Consultancy Ltd took out targeted dark social ads aimed at Conservative Members, accusing some of them of being Brexit mutineers when they had the temerity to vote for common sense in a vote on Brexit in this House. Voter Consultancy Ltd, for those who have not studied its financial records at Companies House, as I have, is a dormant company. It has no accounts filed. There is no cash flowing through the books. The question that provokes is: where does the money come from for the dark social ads attacking Conservative Members? We do not know. It is a matter of public concern that we should.

The law is out of date and needs to be updated. I will not press the matter to a vote this afternoon because I hope to return to it on Report, but I hope that between now and then the Minister and the Secretary of State reflect on the argument and talk to Mark Sedwill, the National Security Adviser, about why the national security strategy does not include an explicit objective to defend the integrity of our democracy. I hope that that change is made and that, as a consequence, further amendments will be tabled to ensure that our democracy is protected against the threats we know are out there.

I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

Question proposed, That the Chair do report the Bill, as amended, to the House.

Margot James: On a point of order, Mr Streeter. I wanted to thank you, and Mr Hanson in his absence, as well as, in the House of Lords, my noble Friends Lord Ashton, Baroness Williams, Lord Keen, Baroness Chisholm and Lord Young, and the Opposition and Cross-Bench peers. I also thank the Under-Secretary of State for the Home Department, my hon. Friend the Member for Louth and Horncastle, and the Opposition Front Bench peers. I offer great thanks to both Whips. It was the first Bill Committee for my hon. Friend the Member for Selby and Ainsty in his capacity as Whip, and my first as Minister, and it has been a pleasure to work with him. I also thank the hon. Member for Ogmore. My hon. Friend the Under-Secretary and I are grateful to our Parliamentary Private Secretary, my hon. Friend the Member for Mid Worcestershire, who has worked terribly hard throughout the proceedings, as indeed have the Clerks, the Hansard writers, the Doorkeepers and the police. Without the officials of my Department and, indeed, the Home Office, we would all have been bereft, and I am most grateful to all the officials.

Question put and agreed to.

Bill, as amended, accordingly to be reported.

3.25 pm

Committee rose.
Written evidence reported to the House

DPB 50 Patrick Daly, Newspaper Conference
DPB 51 Index on Censorship, English PEN, Reporters Without Borders
DPB 52 Richard Parker, Senior Associate, Hill Dickinson LLP

DPB 53 Associated Newspapers
DPB 54 National Union of Journalists
DPB 55 Law Society of Scotland
DPB 56 Curtis Banks Group Plc
DPB 57 Foot Anstey LLP
DPB 58 Nikita Aggarwal