PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

First Sitting

Wednesday 10 May 2023

(Morning)

CONTENTS

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

Sunday 14 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

† Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
† Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Eastwood, Mark *(Dewsbury)* (Con)
Henry, Darren *(Broxtowe)* (Con)
† Hunt, Jane *(Loughborough)* (Con)
† Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Monaghan, Carol *(Glasgow North West)* (SNP)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
† Richards, Nicola *(West Bromwich East)* (Con)
Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

† **attended the Committee**

Witnesses

John Edwards, Information Commissioner, Information Commissioner's Office

Paul Arnold, ICO Deputy Chief Executive and Chief Operating Officer, Information Commissioner's Office

Eduardo Ustaran, Global co-head of the Hogan Lovells Privacy and Cybersecurity practice, Hogan Lovells

Vivienne Artz OBE

Bojana Bellamy, President, Centre for Information Policy Leadership

Neil Ross, Associate Director for Policy, TechUK

Chris Combemale, CEO, Data and Marketing Association

Dr Jeni Tennison OBE, Founder and Executive Director, Connected by Data

Anna Thomas, Co-Founder and Director, Institute for the Future of Work

Michael Birtwistle, Associate Director (AI Law and Regulation), Ada Lovelace Institute

Public Bill Committee

Wednesday 10 May 2023

(Morning)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

9.25 am

The Chair: Before we begin, I have a couple of preliminary announcements that Mr Speaker has asked me to draw to your attention. *Hansard* colleagues would be grateful if Members emailed their speaking notes to hansardnotes@parliament.uk. Please switch electronic devices to silent. Tea and coffee are not allowed during sittings.

Today we will first consider the programme motion on the amendment paper. We will then consider a motion to enable the reporting of written evidence for publication and a motion to allow us to deliberate in private about our questions before the oral evidence session. In view of the time available, I hope we can take these matters formally—without debate. The programme motion was discussed yesterday by the Programming Sub-Committee for this Bill.

Ordered,

That—

1. the Committee shall (in addition to its first meeting at 9.25 am on Wednesday 10 May) meet—

(a) at 2.00 pm on Wednesday 10 May;

(b) at 9.25 am and 2.00 pm on Tuesday 16 May;

(c) at 11.30 am and 2.00 pm on Thursday 18 May;

(d) at 9.25 am and 2.00 pm on Tuesday 23 May;

(e) at 9.25 am and 2.00 pm on Tuesday 6 June;

(f) at 11.30 am and 2.00 pm on Thursday 8 June;

(g) at 9.25 am and 2.00 pm on Tuesday 13 June;

2. the Committee shall hear oral evidence in accordance with the following Table:

Date	Time	Witness
Wednesday 10 May	Until no later than 9.55 am	Information Commissioner's Office
Wednesday 10 May	Until no later than 10.25 am	Hogan Lovells; London Stock Exchange Group; Centre for Information Policy Leadership
Wednesday 10 May	Until no later than 10.50 am	techUK; Data & Marketing Association
Wednesday 10 May	Until no later than 11.25 am	Connected by Data; Institute for the Future of Work; Ada Lovelace Institute
Wednesday 10 May	Until no later than 2.25 pm	Medtronic; UK Biobank
Wednesday 10 May	Until no later than 2.50 pm	ZILO; UK Finance
Wednesday 10 May	Until no later than 3.05 pm	Better Hiring Institute
Wednesday 10 May	Until no later than 3.30 pm	National Crime Agency; Metropolitan Police
Wednesday 10 May	Until no later than 3.55 pm	Prospect; Trades Union Congress
Wednesday 10 May	Until no later than 4.25 pm	Public Law Project; Law Society of Scotland; Rights and Security International
Wednesday 10 May	Until no later than 4.40 pm	AWO

3. proceedings on consideration of the Bill in Committee shall be taken in the following order: Clauses 1 to 5; Schedule 1; Clause 6; Schedule 2; Clauses 7 to 11; Schedule 3; Clauses 12 to 20; Schedule 4; Clause 21; Schedules 5 to 7; Clauses 22 to 41; Schedule 8; Clauses 42 to 45; Schedule 9; Clauses 46 to 86; Schedule 10; Clauses 87 to 98; Schedule 11; Clause 99; Schedule 12; Clause 100; Schedule 13; Clauses 101 to 114; new Clauses; new Schedules; remaining proceedings on the Bill;

4. the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Tuesday 13 June.—*(Sir John Whittingdale.)*

Resolved,

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

Resolved,

That, at this and any subsequent meeting at which oral evidence is to be heard, the Committee shall sit in private until the witnesses are admitted.—*(Sir John Whittingdale.)*

The Chair: Copies of written evidence that the Committee receives will be made available in the Committee Room and circulated to Committee members by email. We will now go into private session to discuss lines of questioning.

9.27 am

The Committee deliberated in private.

Examination of Witnesses

9.30 am

John Edwards and Paul Arnold gave evidence.

The Chair: We are now sitting in public again and the proceedings are being broadcast. Before we hear from the witnesses, do any Members wish to make a declaration of interest in connection with the Bill?

Jane Hunt (Loughborough) (Con): I am not sure whether this is a declaration of interest, so I will mention it just in case. I have had a meeting with Leicestershire Police Federation and I am interested in an amendment that it would like tabled.

Damian Collins (Folkestone and Hythe) (Con): I am not sure whether this is directly relevant to the Bill or adjacent to it, but I am an unpaid member of the board of the Centre for Countering Digital Hate, which does a lot of work looking at hate speech in the online world.

Mark Eastwood (Dewsbury) (Con): Given that one of today's witnesses is from Prospect, I wish to declare that I am a member of that union.

Stephanie Peacock (Barnsley East) (Lab): I am a proud member of a trade union. I refer the Committee to my entry in the Register of Members' Financial Interests.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): I am a proud member of two trade unions.

Dr Rupa Huq (Ealing Central and Acton) (Lab): Should we declare our membership of any union?

The Chair: My advice is that it is always better to declare.

Dr Huq: Okay. I am a member of Unison, formerly the National and Local Government Officers Association.

Christian Wakeford (Bury South) (Lab): I am also a member of a union.

Mike Amesbury (Weaver Vale) (Lab): I am a member of Unison and the GMB.

The Chair: We will now hear oral evidence from John Edwards, the Information Commissioner, and Paul Arnold, the deputy chief executive and chief operating officer of the Information Commissioner's Office. I remind all Members that questions should be limited to matters within the scope of the Bill, and that we must stick to the timings in the programme order, which the Committee has agreed. For this panel, we have until 9.55 am. Will the witnesses please introduce themselves for the record?

John Edwards: Kia ora! My name is John Edwards. I am the Information Commissioner. I took up the job at the beginning of January last year. I was previously the Privacy Commissioner of New Zealand for eight years.

Paul Arnold: I am Paul Arnold, the deputy chief executive and chief operating officer of the ICO. I took up that position in 2016.

The Chair: May I gently say to the witnesses that this is a big room, so you will need to project your voices so that we can hear your evidence?

Q1 Stephanie Peacock: Good morning and welcome. The Bill creates a new body corporate to replace the corporation sole. What impact, both in the short and long term, do you think that will have on its ability to carry out its functions?

John Edwards: The corporation sole model is fit for a number of purposes. That was the structure that I had back home in New Zealand. For an organisation such as the Information Commissioner's Office, it is starting to buckle under the weight. It will benefit, I think, from the support of a formal board structure, with colleagues with different areas of expertise appointed to ensure that we bring an economy-wide perspective to our role, which as we have heard from the declarations of interest spans almost every aspect of human activity.

There will be some short-term, transitional challenges as we make the transition from a corporation sole to a board structure. We will need to employ a chief executive, for example, as well as getting used to those structures and setting up our new accountability frameworks. But I think, in the longer term, the model proposed in the legislation is well proven across other regulators, both domestically and internationally.

Q2 Stephanie Peacock: I would like to ask about the independence of the ICO as it stands. Do you have any experience of being directed by the Secretary of State in a way that has threatened the regulator's impartial position?

John Edwards: No, I do not.

Q3 Stephanie Peacock: If the Bill is passed in its current form, the Secretary of State—whoever that might be—will have the ability to approve and veto statutory codes of practice produced by the commission, as well as to set out a statement of strategic priorities to which the commission will have to adhere. Do you perceive that having any impact on your organisation's ability to act independently of political direction?

John Edwards: No, I do not believe it will undermine our independence at all. What I think it will do is to further enhance and promote our accountability, which is very important.

To take your first challenge, about codes of conduct, we worked closely with the Department for Digital, Culture, Media and Sport and subsequently the Department for Science, Innovation and Technology to ensure that we got the appropriate balance between the independence of the commission with the right of the Executive and Parliament to oversee what is essentially delegated lawmaking. I think we have got there. It is not a right to veto out of hand; there is a clear process of transparency, which would require the Secretary of State, in the event that he or she decided not to publish a statutory code that we had recommended, to publish their reasons, and those would be available to the House. I do think there is an appropriate level of parliamentary and Executive oversight of what is, as I say, essentially a lawmaking function on the part of the commission.

Q4 Stephanie Peacock: If the Secretary of State can veto a code of practice that the commission has produced regarding the activities of Government, will that not mean that they are, effectively, marking their own homework?

John Edwards: I do not believe so. The code of practice would be statutory—it is only the most serious statutory guidance that we would issue, not the day-to-day opinions that we have of the way in which the law operates. But, also, it is a reflection of the commissioner's view of the law, and a statement as to how he or she will interpret and apply the very general principles. A failure of the Secretary of State to table and issue a proposed code would not affect the way in which the commissioner

discharges his or her enforcement functions. We would still be able to investigate matters and find them in breach, regardless of whether that finding was consistent with the Secretary of State's view of the law.

Q5 Stephanie Peacock: I will come on to a slightly different topic now. The ICO will play a huge role in enforcing the measures in the Bill. Is there enough clarity in the Bill to ensure that the commission is able to do that effectively? For example, are you clear on how the commission will enforce the law surrounding terms like "vexatious" and "excessive" with regards to subject access requests?

John Edwards: Yes. We are in the business of statutory interpretation. We are given a law by Parliament. A term like "vexatious" has a considerable provenance and jurisprudence; it is one that I worked with back home in New Zealand. So, yes, I am quite confident that we will be able to apply those.

Q6 Stephanie Peacock: Linked to that, what about terms like "meaningful human involvement" and "significant decision" with regards to automated decision making?

John Edwards: Sorry, what is your question?

Stephanie Peacock: Parts of the Bill refer to there being "meaningful human involvement" and "significant decisions" within automated decision making. That might be in an application for a mortgage or in certain parts of employment. Do you feel that you can interpret those words effectively?

John Edwards: Yes, of course. You are quite right to point out that those phrases are capable of numerous different interpretations. It will be incumbent on my office to issue guidance to provide clarity. There are phrases in the legislation that Parliament could perhaps look at providing clearer criteria on to assist us in that process of issuing guidance—here I am particularly thinking of the phrase "high risk" activities. That is a new standard, which will dictate whether some of the measures apply.

Stephanie Peacock: That is useful. Thank you.

Q7 Damian Collins: Continuing with that theme, the Bill uses a broader definition of "recognised legitimate interests" for data controllers. How do you think the Bill will change the regime for businesses? What sort of things might they argue they should be able to do under the Bill that they cannot do now?

John Edwards: There is an argument that there is nothing under the Bill that they cannot do now, but it does respond to a perception that there is a lack of clarity and certainty about the scope of legitimate interests, and it is a legitimate activity of lawmakers to respond to such perceptions. The provision will allow doubt to be taken out of the economy in respect of aspects such as, "Is maintaining the security of my system a legitimate interest in using this data?" Uncertainty in law is very inefficient—it causes people to seek legal opinions and expend resources away from their primary activity—so the more uncertainty we can take out of the legislation, the greater the efficiency of the regulation. We have a role in that at the Information Commissioner's Office and you as lawmakers have just as important a role.

Q8 Damian Collins: How would you define that clarity that the Bill is seeking? If a data controller thinks, "Well, if I have legitimate business interests, I can make an excuse for doing whatever I like," that surely is not what the Bill intends. How would you define the clarity that you say the Bill seeks?

John Edwards: You are right that it is the controller's assessment and that they are entitled to make that assessment, but they need to be able to justify and be accountable for it. If we investigate a matter where a legitimate interest is asserted, we would be able to test that.

Q9 Damian Collins: How would you test it?

John Edwards: Well, through the normal process of investigation, in the same way as we do now. We would ask whether this was in the reasonable contemplation of the individual who has contributed their data as a necessary adjunct to the primary business activity that is being undertaken.

Q10 Damian Collins: Does this change things very much? It sounds like you are saying that business may assert it has a legitimate interest, but if you think it does not, you can investigate and take action as the law stands currently, effectively.

John Edwards: Yes, that is right. But the clarity will be where specific categories of legitimate interest are specified in the legislation. Again, that will just take out the doubt, if there is doubt as to whether a particular activity falls within scope.

Q11 Damian Collins: Is more clarity needed about the use of inferred data? Major social media platforms rely on inferred data to drive their recommendation tools and systems. There are then questions about whether inferred data draws on protected data characteristics without user permission. A platform might say that that is part of its recognised legitimate business interests, but users might say that it is an infringement of their data rights. Is that clear enough?

John Edwards: I am afraid that I have to revert to the standard, which is, "It depends." These are questions that need to be determined on a case-by-case basis after examination ex post. It is a very general question that you ask. It depends on what the inferred data is being used for and what it is. For example, my office has taken regulatory action against a company that inferred health status based on purchasing practices. We found that that was unlawful and a breach of the General Data Protection Regulation, and we issued a fine for the practice. Again, the law is capable of regulating inferred data, and there is no kind of carte blanche for controllers to make assumptions about people based on data points, whether collected from or supplied by the individual or not.

Q12 Damian Collins: Your predecessor raised the issue of the use of inferred data among users' protected data characteristics—political opinions, religious beliefs, sexual orientation—and said that, without the user's informed consent, that could not be legal. Do you agree with that?

John Edwards: I am not aware of the statement she made or the context in which she made it, so it is difficult for me to say whether she agreed it. Certainly,

informed consent is not the only lawful basis for a data processing activity and it may be that data about protected activities can be inferred and used in some circumstances. I would be happy to come back to you having checked that quote and to give you my views as to whether I agree with it in the context in which it was made.

Q13 Damian Collins: These are quite important matters because inferred data is such an important part of data processing for major platforms, be it a company assessing someone's attitude to risk and how that affects the way they might use a gambling product, versus taking someone's personal, private information, inferring things from it and making them open to suggestions they may not want to receive without their informed consent. That is a grey area, and I wonder whether you think the Bill provides greater clarity, or you think there needs to be more clarity still.

John Edwards: I think there is sufficient clarity. I am not sure whether the Bill speaks to the point you have just made, but for me the overarching obligation to use data fairly enables us to make assessments about the legitimacy of the kinds of practices you are describing.

The Chair: It is a really tight timetable this morning and we have nine minutes left. The Minister wants to ask some questions and there are three Members from the Opposition. I will call the Minister now. Perhaps you would be kind enough, Minister, to leave time for one question each from our three Members of the Opposition.

Q14 The Minister for Data and Digital Infrastructure (Sir John Whittingdale): Thank you, Mr Hollobone. Good morning, Mr Edwards. Both the structure and powers of your office are going to change as a result of the Bill. Do you believe that the existing structure and the absence of the powers you will gain under the Bill have in any way impeded the carrying out of your functions?

John Edwards: The obligation to investigate every complaint does consume quite a lot of our resources. Can I ask my colleague to make a contribution on this point?

Paul Arnold: As the commissioner says, that duty to investigate all complaints can challenge us in terms of where we need to dedicate the majority of our resources.

To the previous question and answer, our role in trying to provide or maximise regulatory certainty means being able to invest as much resource as we can in that upstream advice, particularly in those novel, complex, finely balanced, context-specific areas. We are adding far more value if we can add that support upstream.

The additional statutory objectives that are being added through the Bill overall will be a real asset to our accountability. Any regulator that welcomes independence also needs to welcome the accountability. It is the means through which we describe how we think, how we act and the outcomes that we achieve. Those extra statutory objectives will be a real aid to us and also an aid to Parliament and our stakeholders. It really does crystallise and clarify why we are here and how we will prioritise our efforts and resources.

Q15 Sir John Whittingdale: In the interests of time, I will ask you one other question. Mr Edwards, you had experience as the New Zealand Privacy Commissioner for some time. New Zealand is one of the countries recognised as having data adequacy by the European Union. Can you give us a view, based on your experience of dealing with the European Union, of whether there is any concern about the Bill that might put at risk the UK's data adequacy recognition from the EU?

John Edwards: I do not believe there is anything in the Bill that would put at risk the adequacy determination with the European Union. The test the Commission applies is whether the law is essentially equivalent. New Zealand lacks many of the features of the GDPR, as do Israel and Canada, each of which has maintained adequacy status. The importance of an independent regulator is preserved in this legislation. All the essential features of the UK GDPR or the rights that citizens of the European Union enjoy are present in the Bill, so I do not believe that there is a realistic prospect of the Commission reviewing negatively the adequacy determination.

The Chair: It is a brutal cut-off, I am afraid, at 9.55 am. I have no discretion in this matter. It is a quick-fire round now, gentlemen. We need quick questions and quick answers, with one each from Carol Monaghan, Chi Onwurah and Mike Amesbury.

Q16 Carol Monaghan (Glasgow North West) (SNP): Clause 40 sets out the criteria by which a data controller can refuse data access requests. Do you think this is appropriate? Are you concerned that it may lead to a situation in which only those who can afford to pay a potential fee will be able to access their data?

John Edwards: Yes and no. Yes, I do believe it is an adequate provision, and no, I do not believe there will be an economic barrier to people accessing their information rights.

Q17 Chi Onwurah: The Bill's intent is to reduce burdens on organisations while maintaining high data protection standards. Do you agree that high data protection standards are promoted by well-informed and empowered citizens? What steps do you think the Bill takes to ensure greater information empowerment for citizens?

John Edwards: Yes, I do believe that an empowered citizenry is best placed to enjoy these rights. However, I also believe that the complexity of the modern digital environment creates such an information asymmetry that it is important for strong advocates such as the Information Commissioner's Office to act as a proxy on behalf of citizenry. I do not believe that we should devolve responsibility to citizens purely to ensure that high standards are set and adhered to in digital industries.

Q18 Mike Amesbury: Drawing on your expertise, is there anything missing from the Bill that you would have liked to see?

John Edwards: I do not believe so. We have been involved right from the outset. We made a submission on the initial White Paper. We have worked closely with officials. We have said that we want to see the Bill get to a position where I, as Information Commissioner, am able to stand up and say, "I support this legislation." We have done that, which has meant we have achieved quite significant changes for the benefit of the people of the United Kingdom. It does not mean that we have just accepted what the Government have handed out. We

have worked closely together. We have acted as advocates, and I believe that the product before you shows the benefits of that.

The Chair: We have a late entry—the last question will be from Rupa Huq.

Q19 Dr Huq: When I was on the Criminal Finances Bill Committee, lots was promised, but the National Crime Agency then claimed that it was not financed enough to pursue all the unexplained wealth orders that were promised. Do you think that a beefed-up Information Commission will be sufficiently well resourced to do all the things it is meant to do?

John Edwards: In short, yes. We are having discussions about the funding model with DSIT. We are funded by levies. There are two questions: one is about how those levies are set and where the burden of funding our office lies in the economy, and the second is about the overall quantum. We can always do more with more. If you look at the White Paper on artificial intelligence and the Vallance report, you will see that there is a role for our office to patrol the new boundaries of AI. In order to do that, we will have to be funded appropriately, but I have a good relationship with our sponsor Department and am confident that we will be able to discharge all the responsibilities in the Bill.

The Chair: Gentlemen, thank you very much indeed for your evidence. You can now breathe, relax and enjoy the rest of your day.

Examination of Witnesses

Eduardo Ustaran, Vivienne Artz and Bojana Bellamy gave evidence.

9.53 am

Q20 The Chair: We will now hear oral evidence from Eduardo Ustaran, global co-head of the privacy and cyber-security practice at Hogan Lovells, who is appearing via Zoom; Vivienne Artz OBE, who is in the room; and Bojana Bellamy, president of the Centre for Information Policy Leadership, who is also appearing via Zoom. For this session we have until 10.25 am. Will the witnesses introduce themselves for the record, starting with Vivienne Artz?

Vivienne Artz: Good morning. My name is Vivienne Artz. I am the chair of the International Regulatory Strategy Group data committee, I have more than 25 years' experience in financial services, including acting as a chief privacy officer, and I now do advisory work across a range of sectors, including in the context of financial crime.

The Chair: Will Eduardo Ustaran please introduce himself? Can you hear us, Mr Ustaran? No. Can you hear us, Bojana Bellamy? No. Okay, we will start with our witness who has been kind enough to join us in the room.

Q21 Stephanie Peacock: Welcome. Vivienne, would you be in favour of implementing a smart data regime in your industry? If so, why?

Vivienne Artz: Yes, we are interested in implementing a smart data regime because it will allow broader access to data for innovation, particularly in the context of open banking and open finance. It would require access to information, which can often be limited at the moment. There is a lot of concern from businesses around whether or not they can actually access data. Some clarification on what that means, in respect of information that is not necessarily sensitive and can be used for the public good, would be most welcome. Currently, the provisions in the legislation are pretty broad, so it is difficult to see what it will look like, but in theory we are absolutely in favour.

Q22 Stephanie Peacock: Could you give more detail on who you think would benefit or lose out, and in what ways?

Vivienne Artz: Consumers would absolutely benefit, and that is where our priority needs to be—with individuals. It is an opportunity for them to leverage the opportunities that the data can provide. It will enable innovators to produce more products and services that will help individuals to better understand their financial and personal circumstances, particularly in the context of utility bills and so on. There are a number of positive use cases. There is obviously always the possibility that data can be misused, but I am a great advocate of saying that we need to find the positive use cases and allow business to support society and our consumers to the fullest extent. That is what we need to support.

Q23 Stephanie Peacock: Brilliant. What are your thoughts on giving the Secretary of State the power to amendment data protection legislation further? Do you think it is necessary to future-proof the Bill?

Vivienne Artz: It is necessary to future-proof the Bill. We are seeing such an incredible speed of innovation and change, particularly with regard to generative artificial intelligence. We need to make sure that the legislation remains technology-neutral and can keep up to date with the changes that are currently taking place.

Stephanie Peacock: I have more questions if our other witnesses are with us.

The Chair: We still have not heard definitively whether our other guests can hear us or speak to us, so we are waiting for confirmation from the tech people. In the meantime, I invite the Minister to question Vivienne Artz.

Q24 Sir John Whittingdale: You have a lot of experience in respect of international data transfers. The European Union has a number of data adequacy agreements around the world, but the process to establish them has been slow. How do you think the Bill will make it easier for us to improve international data agreements? What prospects are there for the UK to establish such agreements, and with which countries?

Vivienne Artz: The Bill provides for the opportunity for the Government to look at a range of issues and to move away from an equivalence approach to one in which we can consider more factors and features. The reality is that if you compare two pieces of legislation, you will always find differences because they come from different cultural backgrounds and different legal regimes. There will always be differences. The approach the UK is taking in the Bill is helpful because it looks at outcomes and broader issues such as the rule of law in different jurisdictions.

What is said on paper is not necessarily what always happens in practice; we need to look at it far more holistically. The legislation gives the Government the opportunity to take that broader and more common-sense view with regard to adequacy and not just do a word-by-word comparison of legislative provisions without actually looking at how the legislation is implemented in that jurisdiction and what other rights can support the outcomes. We can recognise that there is a different legal process and application but ask whether it still achieves the same end. That is what is really important. There is an opportunity not only to move more quickly in this space but to consider jurisdictions that might not be immediately obvious but none the less still offer appropriate safeguards for data.

Q25 Sir John Whittingdale: Obviously it is already possible for us to undertake international data transfers to countries with which we do not have an adequacy agreement. Can you set out the advantages of having a general adequacy agreement in terms of data transfer and the benefits to the UK economy?

Vivienne Artz: The current process is incredibly cumbersome for businesses and, if I am honest, it provides zero transparency for individuals as well. It tends to be mostly a paperwork exercise—forgive if that sounds provocative, but putting in place the model clauses is very often an expensive paperwork exercise. At the moment, it is difficult, time-consuming and costly, as the case may be.

The thing with adequacy is that it is achieved at a Government-to-Government level. It is across all sectors and provides certainty for organisations to move forward to share information, sell their goods and services elsewhere and receive those goods and services, and for consumers to access those opportunities as well. Adequacy is certainly the ideal. Whether it is achievable in all jurisdictions I do not know, but I think it is achievable for many jurisdictions to provide confidence for both consumers and businesses on how they can operate.

Sir John Whittingdale: Thank you.

The Chair: We can see Mr Ustaran and Ms Bellamy and they can hear us, but we cannot hear them, so we will carry on with questioning Vivienne Artz.

Q26 Carol Monaghan: A number of organisations have expressed concerns about moving to a situation in which we can refuse subject access requests or indeed charge a fee. Do you believe the thresholds in the Bill are appropriate and proportionate?

Vivienne Artz: I do think the thresholds are appropriate and proportionate. In practice, most organisations do not actually choose to charge, because actually it costs more to process the cheque than it is worth in terms of the revenue. Certainly, some sectors have been subject to very vexatious approaches through claims-management companies and others, where it is a bombarding exercise and it is unclear whether it is in the best interests of the consumers, or whether it is at their understanding and behest, to make a genuine subject access request.

I am a great supporter of subject access requests—they are a way for individuals to exercise their rights to understand what data is being processed—but as a result of quirks of how we operate often in the UK, they are being used as a pre-litigation investigative tool on the cheap, which is unfortunate and has meant that we have had to put in place additional safeguards to ensure they are used for the purpose for which they were provided, which is so that individuals can have transparency and clarity around what data is being processed and by whom.

Q27 Carol Monaghan: Do you think the threshold for something to be considered vexatious or excessive is well understood?

Vivienne Artz: We have heard from the Information Commissioner that they are fairly clear on what that terminology means and it will reflect the existing body of law in practice. I will be perfectly honest: it is not immediately clear to me, but there is certainly a boundary within which that could be determined, and that is something we would rely on the Information Commissioner to provide further guidance on. It is probably also likely to be contextual.

Q28 Carol Monaghan: How frequently do we expect such requests to be refused off the back of this legislation?

Vivienne Artz: I think it depends on the sector. I come from the financial services sector, so the types of subject access requests we get tend to be specific to us. I think organisations are going to be reluctant to refuse a subject access request because, at the end of the day, an individual can always escalate to the Information Commissioner if they feel they have been unfairly treated. I think organisations understand their responsibility to act in the best interests of the individual at all times.

Q29 The Chair: Ms Bellamy and Mr Ustaran, we can now hear both of you. Would you be kind enough to introduce yourselves?

Bojana Bellamy: Thank you for inviting me to this hearing. My name is Bojana Bellamy. I lead the Centre for Information Policy Leadership. We are a global data privacy and data policy think-and-do-tank operating out of London, Brussels and Washington, and I have been in the world of data privacy for almost 30 years.

Eduardo Ustaran: Good morning. My name is Eduardo Ustaran. I am a partner at Hogan Lovells, based in London, and I co-lead our global privacy and cyber-security practice, a team of over 100 lawyers who specialise in data protection law all over the world.

The Chair: Thank you. Chi Onwurah and Damian Collins are lined up to ask questions, but I want first to ask the shadow Minister whether she has any further questions, followed by the Minister. Because we have one witness in the room and two online, please will whoever is asking the question indicate whom you are asking it of?

Q30 Stephanie Peacock: Good morning to our guests joining us via Zoom. Ms Bellamy, in your opinion has it been difficult for businesses to adapt to the EU GDPR? If so, do you think the changes in the Bill will make it easier or harder for businesses to comply with data protection legislation?

Bojana Bellamy: Yes, certainly it has been hard to get businesses to comply with GDPR, in particular small and medium-sized businesses. I think the changes proposed in the Bill will make it easier, because it is more about

outcomes-based regulation. It is more about being effective on the ground, as opposed to being prescriptive. GDPR is quite prescriptive and detailed. It tells you how to do things. In this new world of digital, that is not very helpful, because technology always goes in front of and faster than the rules.

In effect, what we see proposed in the Bill is more flexibility and more onus on organisations in both the public and private sector to deliver accountability and effective protection for people. It does not tell them and prescribe how exactly to do that, yet they are still accountable for the outcomes. From that perspective, it is a step forward. It is a better regime, in my opinion.

Q31 Stephanie Peacock: Mr Ustaran, what do you perceive the value of EU adequacy to be? What would be the consequences for your businesses and other businesses and the UK market of losing such an agreement?

Eduardo Ustaran: From the point of view of adequacy, it is fundamental to acknowledge that data flows between the UK and the EU and the EU and the UK are essential for global commerce and for our digital existence. Adequacy is an extremely valuable element of the way in which the current data protection regime works across both the EU and the UK.

It is really important to note at the outset that the changes being proposed to the UK framework are extremely unlikely to affect that adequacy determination by the EU, in the same way that if the EU were to make the same changes to the EU GDPR, the UK would be very unlikely to change the adequacy determination of the EU. It is important to appreciate that these changes do not affect the essence of UK data protection law, and therefore the adequacy that is based on that essence would not be affected.

Q32 Stephanie Peacock: You have answered my next question—thank you—but I will pose it to the other witnesses, who may have something to add. In the previous session, the Information Commissioner said that he did not think the Bill was a threat to adequacy. That is comforting, but it is not confirmation, because the only people who have the power to decide whether adequacy stands are the European Commission. Do you think any of the measures in the Bill pose a risk to the adequacy agreement?

Bojana Bellamy: I certainly agree that adequacy is a political decision. In many ways—you have seen this with the Northern Ireland protocol—some of these decisions are made for different purposes. I do not believe there are elements of the Bill that would reduce adequacy; if anything, the Bill is very well balanced. Let me give you some examples of where I think the Bill goes beyond GDPR: certainly, on expectations of accountability on the senior responsible individual, which actually delivers better oversight and leadership over privacy; on the right to complain to an organisation and on organisations to respond to these complaints; and on the strong and effective Information Commissioner, who actually has more power. The regulator is smarter; that, again, is better than GDPR. There are also the safeguards that exist for scientific research and similar purposes, as well as some other detailed ones.

Yes, you will see, and you have seen in public projects as well, that there are people who are worried about the erosion of rights, but I do not believe that exception to subject access requests and other rights we talked about are actually a real erosion. I think it just clarifies what has been the law. Some of the requirements to simplify privacy impact assessment and records of processing will, in fact, deliver better accountability in practice. They are still there; they are just not as prescriptive. The Information Commissioner has strong powers; it is a robust regulator, and I do not believe its independence will be dented by this Bill. I say to those who think that we are reducing the level of protection that, actually, the balance of all the rules is going to be essential equivalency to the EU. That is really what is important.

May I say one more thing quickly? We have seen the EU make adequacy decisions regarding countries such as Japan and Korea, and even privacy shield. Even in these cases, you have not had a situation where the requirements were essentially equivalent. These laws are still different from GDPR—they do not have the right of portability or the concept of automated decision making—but they are still found to be adequate. That is why I really do not believe that this is a threat. One thing we have to keep absolutely clear and on par with the EU is Government access to data for national security and intelligence purposes. That is something the EU will be very interested in to ensure that that is not where the bar goes down, but there is no reason to believe so and there is nothing in the Bill to tell us so.

Vivienne Artz: I concur; I do not think the Bill poses any threat to adequacy with the EU. With regard to the national security issue that Bojana raises, I would also point out that the UN rapporteur noted that the UK has better protections for Government access to data than many EU member states, where it is often a very political approach as opposed to a practical approach and really looking at what the outcomes are. There is nothing in this Bill that would jeopardise adequacy with the EU.

The Chair: We have 12 minutes left and two Members are indicating that they wish to ask questions after you, Minister.

Q33 Sir John Whittingdale: I will be very quick, Mr Hollobone. Ms Bellamy, you have suggested that in some ways the regime that the Bill puts in place is superior to that of the existing GDPR and that it certainly does not risk our adequacy recognition in any way. Given the development of technology and the increasing use of things like AI, to what extent do you think the EU might follow the same sort of path that the Bill sets out to try to create a more flexible and a state-of-the-art regime?

Eduardo Ustaran: That is a very important question to address because perhaps one of the ways in which we should be looking at this legislative reform is a way of seeing how the existing GDPR framework that exists both in the EU and the UK could, in fact, be made more effective, relevant and modern to deal with the issues we are facing right now. You refer to artificial intelligence as one of those issues.

GDPR in the EU and the UK, is about five years old. It is not a very old piece of legislation, but a number of technological developments have happened in the past five years. More importantly, we have learned how GDPR operates in practice. This exercise in the UK is in fact very useful, not just for the UK but for the EU

and the world at large, because it is looking at how to reform elements of existing law that is already in operation in order to make it more effective. That does not mean that the law needs to be more onerous or more strict, but it can be more effective at the same time as being more pragmatic. This is an important optic in terms of how we look at legislative reform, and not only from the UK's point of view. The UK can make an effort to try to make the changes more visible outside the United Kingdom, and possibly influence the way in which EU GDPR evolves in the years to come.

Bojana Bellamy: I agree that we need a more flexible legal regime to enable the responsible use of AI and machine learning technologies. To be very frank with you, I was hoping the Bill would go a little further. I was hoping that there would be, for example, a recognition of the use of data in order to train algorithms to ensure that they are not discriminatory, not biased and function properly. I would have hoped that would be considered as an example of legitimate interests. That is certainly a way in which the Government can go further, because there are possibilities for the Secretary of State to augment those provisions.

We have seen that in the European AI Act, where they are now allowing greater use of data for algorithmic AI training, precisely in order to ensure that algorithms work properly. We have Dubai's data protection law and some others are starting to do that. I hope that we have good foundations to ensure further progression of the rules on AI. The rules on automated decision making are certainly better in this Bill than they are in GDPR. They are more realistic; they understand the fact that we going to be faced with AI and machine learning taking more and more decisions, of course with the possibility of human intervention.

Again, to those who criticise the rules, I would say it is more important to have these exposed rights of individuals. We should emphasise, in the way we have done in the Bill, the right to information that there is AI involved, the right to make a representation, the right to contest a decision, and the right to demand human review or human intervention. To me, that is really what empowers individuals and gives them trust that the decisions will be made in a better way. There is no point in prohibiting AI in the way GDPR sort of does. In GDPR, we are going to have something of a clash between the fact that the world is moving toward greater use of AI, and that in article 22 on automated decision making, there is a prohibition that makes it subject to consent or contract. That is really unrealistic. Again, we have chosen a better way.

As a third small detail, I find the rules on research purposes to be smarter. They are rather complicated to read, to be frank, but I look forward to the consolidated, clean version. The fact that technological development research is included in commercial research will enable the organisations that are developing AI to create the rules in a responsible way that creates the right outcomes for people, and does not create harms or risks. To me, that is what matters. That is more important, and that is what is going to be delivered here. We have the exemptions from notices for research and so on, so I feel we will have better conditions for the development of AI in a responsible and trusted way. However, we must not take our eyes off it. We really need to link GDPR with our AI strategy, and ensure that we incentivise organisations to be accountable and responsible when they are developing and deploying AI. That will be a part of the ICO's role as well.

The Chair: Five minutes left. This will be the quick-fire round. I have two Members indicating that they wish to ask questions—Chi Onwurah.

Q34 Chi Onwurah: Thank you, Mr Hollobone. We have heard that the intent in the Bill is in part to reduce the burden on organisations from data protection. We heard you set out what some of those burdens might be. The organisations affected by this Bill, and the organisations with which you work in different ways, operate in different jurisdictions. I think you, Ms Artz, set out quite well the challenges of having—or trying to have—the same regime in different jurisdictions. If forced to make a choice between following the European Union regime and following a divergent UK regime, what choice would the organisations with which you work make?

The Chair: Please choose one witness.

Chi Onwurah: Mr Ustaran, please.

Eduardo Ustaran: This is a question that many organisations that operate globally face right now. You must understand that data protection law operates all over the world and data flows all over the world, so consistency is really important in order to achieve compliance in an effective way. Therefore, a question—a very valid question—is, "Do I comply with the EU GDPR across the board, including in the UK, or should I make a difference?"

The reality is that when you look at the way in which the UK data protection framework is being amended, it provides a baseline for compliance with both the UK and EU regimes, in the sense that much of what is being introduced could potentially be interpreted as already being the case in the EU, if you apply perhaps a more progressive interpretation of EU law. Therefore, I think we should look just a little bit further than just saying, "Well, if I do comply with EU law, will I be all right in the UK?"

Maybe the way to look at it—something I see some organisations exploring—is, "If I were to take the UK interpretation of the GDPR on a wholesale basis, would that allow me to operate across the world, and certainly in the EU, in a more effective and efficient but still compliant way?" This is something that companies will be exploring, and it is not as easy as simply saying, "Well, I will just do EU law across the board."

Chi Onwurah: Could I—

The Chair: Sorry. It must be one quick question and one quick answer. We must finish at 10.25 am. Damian Collins.

Q35 Damian Collins: Ms Artz, one of the complaints about the current GDPR regime has been, for example, that oligarchs use it aggressively to target investigative journalists conducting legitimate investigations into their business activities, to bombard them with data access requests. Do you think that the provisions in the Bill around vexatious requests will help in that situation? Do you think that it will make any difference?

Vivienne Artz: I think it will help a little bit in terms of the threshold of "vexatious". I think the other piece that will help is the broadening of the provisions around legitimate interests, because now there is an explicit legitimate interest for fraud detection and prevention. At the moment, it is articulated mostly as to prevent a crime. I would suggest that it could be broadened in the context of financial crime, which has anti-money laundering, sanctions screening and related activities, so that firms can actually process data in that way.

Those are two different things: the one is processing data around sanctioned individuals and such like in the context of suspicious activities, and the other is the right of a subject access to remove their data. Even if they make that subject access request, the ability now to balance it against broader obligations where there is a legitimate interest is incredibly helpful.

The Chair: I thank all three witnesses for their time this morning and their extremely informative answers to the questions. Our apologies from Parliament for the tech issues that our two Zoom contestants had to endure. Thank you very much indeed. We will now move on to our third panel.

Examination of Witnesses

Neil Ross and Chris Combemale gave evidence.

10.25 am

Q36 The Chair: Welcome. We will now hear oral evidence from Neil Ross, Associate Director for Policy at techUK, and Chris Combemale—I hope I pronounced that correctly—the Chief Executive Officer of the Data and Marketing Association. Gentlemen, this session, as you have seen from the previous two, has to end no later than 10.50 am. I will be grateful if you could be kind enough, please, to introduce yourselves to the Committee for the record.

Neil Ross: Thank you for having us before the Committee. My name is Neil Ross. I am the Associate Director for Policy at techUK, the trade association that represents the technology sector in the UK. We have 950 companies in our membership.

Chris Combemale: I am Chris Combemale, the CEO of the Data and Marketing Association. I have 40 years' experience as a practitioner in marketing and advertising. I started on the agency side, including well-known brands, leading marketing technology business and first-generation cloud marketing technology.

The Chair: I apologise for getting your surname pronunciation wrong, Mr Combemale.

Chris Combemale: That's okay, it happens all the time. It is actually of French heritage, rather than Italian.

Q37 Stephanie Peacock: Welcome to the witnesses. TechUK's response to the withdrawn Bill last autumn stated that it

"could go further in seeking the full benefits of data driven innovation".

Does this amended Bill go further?

Neil Ross: Yes, it does. If we go back to the statement of the Information Commissioner earlier, the most important part of the legislation is to provide increased clarity on how we can use data. I think there were about 3,000 responses to the consultation, and the vast majority—particularly around the scientific research and the legitimate interest provisions—focused on providing that extra level of clarity. What the Government have done is quite clever, in that they have lifted examples from the recitals—recital 157, as well as those related to legitimate interests—to give additional clarity on the face of the Bill, so that we can take a much more innovative approach to data management and use in the UK, while still maintaining that within the broad umbrella of what means we qualify for EU adequacy.

Q38 Stephanie Peacock: How have your members found adapting to GDPR? Will the Bill make it easier or harder for those that you represent to comply?

Neil Ross: Most tech companies have adapted to GDPR. It is now a common global standard. The Bill makes the compliance burden a little easier to use, allows us to be a little more flexible in interpretation of it and will give companies much more certainty when taking decisions about data use.

One really good example is fraud. Online fraud is a massive problem in the UK and the Government have a strategy to deal with it, so having that legitimate interest that focuses on crime prevention—also those further processing rights around compliance with the law—means that we can be much more innovative and adaptive about how we share and process data to protect against and prevent fraud. That will be absolutely vital in addressing the shared objective that we all have to reduce online fraud.

Q39 Stephanie Peacock: On the changes to requirements to report suspicious activity related to unsolicited direct marketing, do the telecoms companies among your members have the technical capability to identify instances of mass unsolicited direct marketing in order to report as required?

Neil Ross: No. That is one area where we think further work is needed in the Bill. I think you are referring to clause 85. When we responded to the consultation, we said that the Government should try to create equivalence between the private communications requirements and the GDPR to give that extra level of flex. By not doing that and by not setting out specific cases of where telecoms companies have to identify unsolicited calls, the Government are being really unfair in what they are asking them to do. We have had concerns raised by a range of companies, both large and small, that they might not have the technical capability and that they will have to set up new systems to do it. Overall, we think that the Bill makes a bit of a misstep here and that we need to clarify exactly how it will work. TechUK and some of my colleagues will be suggesting to the Committee some legal amendments for how to do that.

Q40 Stephanie Peacock: On that point, do the telecoms companies feel that they have been consulted properly in the making of the legislation?

Neil Ross: No, not on that clause, but yes in relation to the rest of the legislation.

Q41 Stephanie Peacock: I was asking about that. Chris, will the changes to the cookies set out in the Bill benefit, first, the consumer experience and, secondly, your members or businesses?

Chris Combemale: Yes. First, on the consumer experience, I think that we all recognise that the pop-up consent banners for cookies are generally ticked as a matter of course by consumers who really want to go about their business and get to the website that they want to do business on. In a way, it is not genuine consent, because people are not really thinking deeply about it.

In terms of business, a number of the cookies, which are really identifiers that help you understand what people are doing on your website, are used just on a first-party basis by websites, such as e-commerce websites and business-to-business websites, to understand the basic operational aspects and statistical measurement of how many people are going to which pages. Those are websites that do not take any advertising and do not share any data with third parties, so the exemptions in the Bill generally would make those types of companies no longer need cookie banners while providing no risk to the customers, because the company uses the cookies purely to understand the behaviours of its own website traffic and its own customers. In that sense, we strongly support the provisions and the exemptions in the Bill.

Q42 Stephanie Peacock: Is the technology available to centralise cookies by browser?

Chris Combemale: I think it can be eventually, but we oppose those provisions in the Bill, because they create a market imbalance and give control as a gateway to large companies that manage browser technology, at the expense of media owners and publishers that are paying journalists and investing in content. It is incumbent upon all else that media owners are able to develop first-party relationships with their audiences and customers to better understand what they need. If anything, we need more control in the hands of the people who invest in creating the content and in paying the journalists who provide those important democratic functions.

Q43 Stephanie Peacock: Is there a concern that centralising cookies by browser will entrench power in the hands of the larger tech companies that own the browsers?

Chris Combemale: It certainly would give even greater market control to those companies.

Q44 Stephanie Peacock: Is the risk in centralising cookies by browser that we could confuse liability, for example who is responsible for a breach of cookie regulation?

Chris Combemale: I think it could be. For us, the essential principle is that a business, whether a media owner, e-commerce business or publishing business, should have control of the relationships between its products and services and its customers and prospects for its customers. By nature, when you give control to a third party, whether a large tech company or another company, you are getting in between the relationship between people and the organisations that they want to do business with and giving control to an intermediary who may not understand. At the least point, if you register with a website after, for instance, changing your browser setting, that should take precedence over the browser setting: your choice to engage with a particular company should always take precedence over a centralised cookie management system.

Neil Ross: I think that what the Government have done in relation to this is quite clever: they have said that their objective is to have a centralised system in the future, but they have recognised that there are a number of different ongoing legislative and regulatory activities that have a significant bearing on that. I think it was only last week that the Government introduced the Digital Markets, Competition and Consumers Bill, clause 20 of which—on conduct requirements—would play a large role in whether you could set up a centralised system, so there is an element of co-ordinating two different but ongoing regulatory regimes. I think we agree with Chris that the steps on analytical cookies now are good but that we need to have a lot more deep thought about what a centralised system may or may not look like and whether we want to go ahead with it.

Chris Combemale: May I come in on that final point? What makes sense to us is a centralised system for managing opt-outs as opposed to managing consent. As the Data and Marketing Association, we operate the telephone preference service and the mailing preference service, which give consumers the opportunity to opt out from receiving unwanted cold calls or unwanted direct mail. There is already a system in place with digital advertising—an icon that people can use to opt out from the use of personal data for personalising digital ads. I think it makes sense that, if people do not want to receive certain things, they can opt out centrally, but a centralised consent opt-in gives too much control to the intermediaries.

Stephanie Peacock: Thank you.

Q45 Sir John Whittingdale: Mr Ross, I know that techUK has been supportive of a number of elements of the Bill, particularly around the opportunities created by the use of smart data. Will you set out your view of the opportunities, and how the Bill will help to attain them?

Neil Ross: Smart data is potentially a very powerful tool for increasing consumer choice, lowering prices and giving people access to a much broader range of services. The smart data provisions that the Government have introduced, as well as the Smart Data Council that they are leading, are really welcome. However, we need to go one step further and start to give people and industries clarity around where the Government will look first, in terms of what kind of smart data provisions they might look at and what kind of sectors they might go into. Ultimately, we need to make sure that businesses are well consulted and that there is a strong cost-benefit analysis. We then need to move ahead with the key sectors that we want to push forward on. Similarly to on nuisance calls, we will send some suggested text to the Committee to add those bits in, but it is a really welcome step forward.

Q46 Sir John Whittingdale: Which particular sectors offer the most opportunity?

Neil Ross: I do not want to name specific sectors at this point. We are having a lot of engagement with our members about where we would like to see it first. The transport sector is one area where it has been used in the past and could have a large use in the future, but it is something that we are exploring. We are working directly

with the Government through the Smart Data Council to try to identify the initial sectors that we could look at.

Q47 Sir John Whittingdale: Thank you. Mr Combemale, will you set out some of the obstacles for your organisation, and how you would like the Bill to reduce them?

Chris Combemale: I think the single biggest one that has troubled our members since the implementation of GDPR is the issue around legitimate interest, which was raised by the hon. Member for Folkestone and Hythe. The main issue is that GDPR contains six bases of data processing, which in law are equal. For the data and marketing industry, the primary bases are legitimate interest and consent. For some reason it has become widely accepted through the implementation of GDPR that GDPR requires consent for marketing and for community activities. I am sure that you hear in your constituencies of many community groups that feel that they cannot go about organising local events because they must have consent to communicate. That has never been the intention behind the legislation; in fact, the European Court of Justice has always ruled that any legal interest could be a legitimate interest, including advertising and marketing.

If you look at what we do, which is effectively finding and retaining customers, the GDPR legislation says in recital 4 that privacy is a fundamental right, not an absolute right, and must be balanced against other rights, such as the right to conduct a business. You cannot conduct a business without the right to find and retain customers, just as you cannot run a charity without the right to find donors and volunteers who provide the money and the labour for your good cause. The clarification is really important across a wide range of use cases in the economy, but particularly ours. It was recognised in GDPR in recital 47. What the legislation does is give illustrative examples that are drawn from recitals 47, 48 and 49. They are not new examples; they are just given main text credibility. It is an illustrative list. Really, any legal interest could be a legitimate interest for the purpose of data providing, subject to necessity and proportionality, which we discussed earlier with the Information Commissioner.

Q48 Carol Monaghan: We have heard already this morning that a number of words and phrases could have some ambiguity associated with them, such as the word "excessive", and the Bill allowing certain cookies that are "low risk". Do you think that the phrase "low risk" is well enough understood?

Chris Combemale: In the sector that I represent, we have a fairly clear understanding of the gradients of risk. As I was saying earlier, many companies do not share data with other companies. They are interested solely in the relationships that they have with their existing customers or prospects. In that sense, all the customer attitudes to privacy research that we do indicates that people are generally comfortable sharing data with companies they trust and do business with regularly.

Q49 Carol Monaghan: Would that then be the definition of low risk?

Chris Combemale: I would not want to suggest what the legal definition is. To us in direct marketing and in the Data and Marketing Association, existing customer relationships—loyal customers who trust and are sometimes passionate about the brands they interact with—are low risk. Higher risk is when you come to share data with other companies, but again much of that activity and data sharing is essential to creating relevance. With the right protections, it is not a hugely high-risk activity. Then you can move on up, so the higher the degree of automation and the higher the degree of third-party data, the greater the risk, and you have to put in place mitigations accordingly. I am not a lawyer—I am just a poor practitioner—so I cannot define it from a legal point of view, but it is clear in the context of our industry how risk elevates depending on what you are doing.

Q50 Carol Monaghan: I might come back to that in a second, but I think Neil wanted to add something.

Neil Ross: I was going to say that you can see how Chris has interpreted it through the lens of his industry, but the feedback we have had from our members, who operate across a range of industries, suggests that there is quite a lot of confusion about what that terminology might mean. The rest of the Bill aims to clarify elements of the GDPR and put them on the face of the Bill, but this provision seems to be going in the other direction. It raises concern and confusion.

That is why our approach has always been that you are going to get more clarity by aligning the Privacy and Electronic Communications Regulation 2003 more with the GDPR, which has clear legal bases, processes and an understanding of what is high and low risk—a balancing test, and so on—than through this fairly broad and poorly understood term "low risk". We have concerns about how it will operate across a range of sectors.

Q51 Carol Monaghan: Chris, you said that you are not a lawyer and cannot define what low risk is, but there will of course have to be some sort of definition. Have we captured that well enough?

Chris Combemale: Coming back to our discussion about legitimate interest and the proportionality balancing test, or legitimate interest impact assessments, when you are thinking about what you are planning to do with your customers, it is a requirement of good marketing without the legislation, but also within the legislation, to think about how what you are planning to do will impact your customers' privacy, and then to mitigate. The important thing is not to say, "There's no risk," "It is low risk," or "It is high risk"; it is to understand that the higher the risk, the greater the mitigations that you have to put in place. You may conclude that you should not do something because the risk level is too high. That is what balancing tests do, and decisions and outcomes result from them.

Q52 Carol Monaghan: The potential difficulty here is that the responsibility is being put on the company. You have described a responsible company that categorises levels of risk and takes action accordingly. Without a clear definition, if it were a less scrupulous company, would there be a grey area?

Chris Combemale: We do a lot of work combating rogue traders, and we provide evidence to cases from our work with the telephone preference service and

other activities. Rogue traders—especially those with criminal intent—will generally ignore the legislation anyway regardless of what you do and whether it lacks clarity or not, but I think you are right. An important part of GDPR is that it puts a lot of responsibility on companies to consider their particular activity, their particular customer base and the nature of their audience. Age UK, a charity that has a lot of vulnerable elderly customers, has to have greater protections and put more thought into how it is doing things than a nightclub marketing to under-30s, who are very technologically literate and digitally conversant.

When we do customer attitudes to privacy studies, we see three broad segmentations—data unconcerned, data pragmatist and data fundamentalist—and they require different treatment. It is incumbent on any company, in a marketing context, to understand who their audience and their customer base is, and design programmes appropriately to build trust and long-term relationships over time. That is an important element of GDPR, from a marketer's perspective. I should add that it should not take legislation to force marketers to do that.

The Chair: There are five minutes left and there are two Members seeking to ask questions.

Q53 Damian Collins: With regards to children's data rights, do you think the Bill will have any implications for the way in which the age-appropriate design code has been implemented by companies working within it at the moment? It is not expressly written into the Bill, but do you expect there to be change?

Neil Ross: No, I do not expect so. Given some of the exemptions for further processing, it might help improve compliance with the law, because compliance with the law in the public interest is then a basis on which you could process data further. It might make it easier for companies to implement the age-appropriate design code.

Q54 Damian Collins: Can you give any examples of that?

Neil Ross: It just gives additional clarity on when and where you can use data on various grounds. There are a wide range of circumstances that you can run into in implementing the age-appropriate design code, so having more flexibility in the law to know that you can process data to meet a legal objective, or for a public interest, would be helpful. The best example I can give is from the pandemic: the Government were requesting data from telecoms companies and others, and those companies were unsure of the legal basis for sharing that data and processing it further in compliance with a Government or regulator request. The Bill takes significant steps to try and improve that process.

Q55 Damian Collins: Could you give an example more directly related to children?

Neil Ross: I do not have one to hand, but we could certainly follow up.

Q56 Mike Amesbury: The Bill enables the commissioner to impose a fine of £1,000. Is that a reasonable deterrent?

Neil Ross: That is in relation to clause 85?

Q57 Mike Amesbury: For non-compliance.

Neil Ross: We do not think it is particularly appropriate for this scenario, given that the telecoms operators are just informing the ICO about activity that is happening on their service. It is not that they are the bad actors in the first instance; they are having to manage it. Ultimately, the first step is to clarify the aims of clause 85, and then whether the fine is appropriate is a subsequent question.

Q58 Mike Amesbury: For some companies, £1,000 will be small fry.

Neil Ross: It will vary from company to company. Most companies will always seek to comply with the law. If you feel you need some kind of deterrent, that is something for Parliament to consider. The first step is to make sure that the law is really clear about what companies are being asked to do. At the moment, that is not the situation we are in.

The Chair: There are two minutes left. Chi Onwurah has the last question.

Q59 Chi Onwurah: Mr Combemale, you set out some of the challenges of having centralised cookie management, and how that would give more power to the browsers. What you did not set out was how we could give more control and power to customers—citizens—over how they use their data. What are you doing to ensure that consumers have more control over how their data is used? You talked about the little thing that you can click to stop our personal data being used—that has been in place for some time now and it is great. If we have the time, Mr Ross, what is your sector doing as well, because the technology should be there to help and empower people?

Chris Combemale: I think a lot of what our sector does voluntarily—setting aside the legislation—is the creation of what are called permission centres. You will be familiar with them from when you go to a website and it asks about categories of information or products that you are interested in. That allows consumers to express their interest. Within the legislation there is very clear data notification, required at the point that data is collected, which requires companies to ask you what you want to do. Whether it is consent or legitimate interest, consumers always have the right to opt out.

With marketing, there is an absolute right to ask not to receive marketing of any kind, whether that is email, direct mail or telephone, at any time. Companies have an obligation to follow that. When it comes to marketing, which is my subject matter expertise, consumers are very well protected and do exercise their rights to opt out. They are further protected by central services, for example the telephone preference service. That is a law that companies can look up; 70% or so of households have registered their telephone number there. I think there are a large number of protections in place, both through the legislation and voluntarily.

Q60 The Chair: Mr Ross, you have 30 seconds.

Neil Ross: There has been a big drive among many tech companies to explain better how they use and handle data practices. There is a drive within the sector to do that anyway. Some of that has come from legislative regulatory activity—for example, the Online Safety Bill and other places.

One thing I would say about this legislation is that it does give people more control over data through the privacy management frameworks. By taking a less strict tick-box approach to data-handling practices, there is the opportunity for core sectors or interest groups such as trade unions to put forward what their ideal data-handling practice should be for a company. As long as that complies with what the ICO sets out or the broad guardrails, then you can see a range of different handling practices adopted, depending on which sector you are in. That flexibility gives some power back to consumers and other interest groups.

The Chair: Gentlemen, you have been brilliant. Thank you very much indeed for your time this morning. We will now move on to the fourth panel.

Examination of Witnesses

10.50 am

Dr Jeni Tennison, Anna Thomas and Michael Birtwistle gave evidence.

Q61 The Chair: We will now hear oral evidence from Dr Jeni Tennison, founder and executive director of Connected by Data; Anna Thomas, co-founder and director at the Institute for the Future of Work; and Michael Birtwistle, associate director of AI law and regulation at the Ada Lovelace Institute. For this session we have until 11.25 am. Will the witnesses, from right to left, please be kind enough to introduce themselves to the Committee for the record?

Dr Tennison: Thank you very much for inviting me here today. My name is Dr Jeni Tennison. I am the executive director of Connected by Data, which is a campaign to give communities a powerful say in decisions about data. Prior to that I was the CEO of the Open Data Institute. I am also the co-chair of the data governance working group in the Global Partnership on Artificial Intelligence.

Anna Thomas: Good morning and thank you for having me. I am Anna Thomas, a founding director of the Institute for the Future of Work, a research and development institute exploring the impact of new technologies on work and working lives. I was formerly an employment barrister at Devereux Chambers. The institute is also the strategic research partner for the all-party parliamentary group on the future of work.

Michael Birtwistle: Good morning. I am Michael Birtwistle, an associate director at the Ada Lovelace Institute, responsible for law and policy. The Ada Lovelace Institute is an independent research institute with a mission to make sure that data and AI work for people and society. I was previously a policy adviser at the Centre for Data Ethics and Innovation.

The Chair: Welcome. Stephanie Peacock will start the questions.

Q62 Stephanie Peacock: Good morning. To go first to Dr Jeni Tennison, do you think the general public and workers have a good level of trust and understanding in terms of how their data is being used? What does the Bill do, if anything, to help build or improve on that trust and understanding?

Dr Tennison: Surveys and public attitudes polling show that when you ask people about their opinions around the use of data, they have a good understanding about the ways in which it is going wrong, and they have a good understanding about the kinds of protections that they would like to see. The levels of trust are not really there.

A poll from the Open Data Institute, for example, shows that only 30% trust the Government to use data ethically. CDEI has described this as "tenuous trust" and highlighted that about 70% of the public think that the tech sector is insufficiently regulated. I do not think that the Bill addresses those issues of trust very well; in fact, it reduces the power individuals have and also the level of collective representation people can have, particularly in the work context. I think this will diminish trust in the way in which data is used.

Q63 Stephanie Peacock: Do you believe the Government have consulted the public and data subjects such as workers appropriately during the process of formulating the Bill?

Dr Tennison: Obviously, there was a strong consultation exercise around the data reform Bill, as it was then characterised. However, there are elements of this Bill, in particular the recognised legitimate interests that are listed, that have not had detailed public consultation or scrutiny. There are also not the kinds of provisions that we would like to see on ongoing consultation with the public on specific questions around data processing in the future.

Q64 Stephanie Peacock: What value do subject access requests hold for citizens, and how will changing the threshold for refusing a request or changing a request to "vexatious or excessive" impact citizens' ability to exercise their rights?

Dr Tennison: Subject access requests are an important way in which citizens can work out what is happening within organisations with the data that is being held about them. There are already protections under UK GDPR against vexatious or excessive requests, and strengthening those as the Bill is doing is, I think, going to put off more citizens from making these kinds of requests.

It is worth noting that this is a specific design of the Bill. If you look at the impact assessment, this is where most of the cost to business is being saved; that is being done by refusing subject access requests. So I think we should be suspicious about what that looks like. Where we have been looking at the role of subject access requests in people exercising their rights, it is clear that that is a necessary step, and delays to or refusals of subject access requests would prevent people from exercising their rights.

We think that a better way of reducing subject access requests would be to have publication of things like the risk assessments that organisations have to do when there is high-risk processing—so that there is less suspicion on the part of data subjects and they do not make those requests in the first place.

Q65 Stephanie Peacock: Thank you. I have a couple of questions for Anna Thomas now. Do the current laws around automated decision making do enough to protect workers and citizens from harm?

Anna Thomas: Referring partly to our work in "Mind the gap" and "The Amazonian Era", as well as the report by the all-party parliamentary group on the

future of work about use of AI in the workplace, we would say no. The aim of the Bill—to simplify—is very good. But particular areas in the Bill as it stands—eroded somewhat—are particularly problematic in the workplace. The automated ones that you ask about are really important with regard to the reduction of human involvement. But in addition to that are the need to assess in advance what the risks and impacts are, the requirement for consultation, and the access to relevant information. Those are all relevant and overlap with the automated decision making requirement.

Q66 Stephanie Peacock: Linked to that, do you believe that the safeguards outlined in the Bill—having a right to human review, for example—are enough to protect workers from the potential harm of automated decision making?

Anna Thomas: Not in themselves. There is potential, in those areas, to correct that or to improve it in the course of the Bill's proceedings, in order that the opportunities, as well as the risks, of putting this new Bill through Parliament are seized. But, no, because of the transformation of work and the extent of the impact, as well as the risks, that new technologies and automated technologies are having across work, not just on access to work, but on terms, conditions, nature, quality and models for work, the safeguards—there is, I think, increasing cross-party consensus about this—should be, in those areas, moving in the other direction.

Q67 Stephanie Peacock: My final question is to Michael. Do you believe that the current regulation does enough to govern the use of biometric technologies?

Michael Birtwistle: No, we would say that it does not. The Ada Lovelace Institute published a couple of reports last year on the use of biometric data, arguing for a much stronger and coherent regulatory governance framework for biometric technologies. These are a set of technologies that are incredibly personal. We are used to their being talked about in terms of our faces or fingerprints, but actually it is a much wider range, involving any measurement to do with the human body, which can be used in emotional analysis—walking style or gait, your tone of voice or even your typing style. There is also a set of incoming, next-generation AI technologies that rely quite heavily on biometrics, so there is a question about future-proofing the Bill.

We have made two broad proposals. One is to increase the capability of the Information Commissioner's Office to look specifically at biometrics—for example, to create and maintain a public register of private entities engaging in processing of biometric data, to have a proper complaints procedure, to publish annual reports and so on. There is a set of issues around increasing the capability of our institutions to deal with that.

Then there is a second question about scope. First, the current focus of biometric data and definition is on identifiability of personal data. There are many potentially problematic use cases of biometric data that do not need to know who you are in order to make a decision about you. We think it would be wise and would future-proof the regulation of this powerful technology to also include classification or categorisation as the purpose of those biometric technologies.

Q68 Damian Collins: You make a very interesting point there, Mr Birtwistle. With automated decision making, a lot of that could be done anonymously. The user is just the end product. They are being targeted through systems and do not need to be identified; the systems just need to know what their data profile is like in order to make a decision.

I am interested in the views of the other members of the panel as well. Do you think there needs to be a greater onus on data controllers to make clear to regulators what data they are gathering, how they are processing it and what decisions are being made based on that data, so that, particularly in an automated environment, while there may not be a human looking at every step in the chain, ultimately a human has designed the system and is responsible for how that system is working?

Michael Birtwistle: I think that is a really important point that is going to be very relevant as we read this Bill alongside the AI White Paper provisions that have been provided. Yes, there is definitely a need for transparency towards regulators, but if we are thinking about automated decision making, you also want a lot of the safeguards and the thinking to be happening within the firms on a proactive basis. That is why the provisions for automated decision making within the Bill are so important. We have concerns around whether the more permissive automated decision making approach in the Bill is actually going to lead to greater harms occurring as, effectively, it turns the making of those automated decisions from a sort of prohibition with exceptions into something that, for anything other than special category data, is permitted with some safeguards, which again there are questions around.

Q69 Damian Collins: On that point, just to be clear, as long as what someone is doing is not clearly and purely illegal, legitimate interest means you can do whatever you want.

Michael Birtwistle: Legitimate interest still has a balancing test within it, so you would not necessarily always be able to show that you had passed that test and to do whatever you want but, certainly, the provisions in the Bill around automated decisions bring legitimate interest into scope as something that it is okay to do automated processing around.

Damian Collins: Dr Tennison?

Dr Tennison: On your first point, around the targets of decisions, one of the things that we would really argue for is changing the sets of people who have rights around automated decision making to those who are the subject of the decisions, not necessarily those who data is known about for those decisions. In data governance practice, we talk about these people as being decision subjects, and we think it is they who should have the rights over being informed about when automated decision making is happening, and other kinds of objection and so forth. That is because, in some circumstances, as you said, there might be issues where you do not have information about someone and nevertheless you are making decisions about them, or you have information about a subset of people, which you are then using to make a decision that affects a group of people. In those circumstances, which we can detail more in written evidence, we really need to have the decision subjects' rights being exercised, rather than the data subjects' rights —those who the data is known about.

On the legitimate interest point you raised, there is this balancing test that Michael talked about, that balances the interests of data subjects as well. We think that there should also be some tests in there that balance public interests, which may be a positive thing for using data, but also may be a negative thing. We know that there are collective harms that arise from the processing of data as well.

Q70 Damian Collins: I just want to make sure I have understood that point correctly. Let us say that someone is a recipient of an advert, not because they have been personally targeted, but because they have been targeted through data-matching tools such as lookalike audiences on Facebook. Would that be the sort of thing you are referring to?

Dr Tennison: Yes, it could be, or because they are using a specific browser, they are in a particular area from their IP or something like that. There are various ways in which people can be targeted and affected by those decisions. But we are not just talking about targeted advertising; we are talking about automated decisions in the workplace or automated decisions about energy bills and energy tariffs. There are lots of these decisions being made all the time.

Q71 Damian Collins: Is the gig economy an example of where the systems are biased towards workers who are always available for jobs, or biased towards people based on their proximity to a particular location for work?

Dr Tennison: Yes. Or they may be subject to things like robo-dismissal, where their performance is assessed and they get dismissed from the job, or they are no longer given jobs in a gig economy situation.

Q72 Damian Collins: Effectively a form of constructive dismissal.

Dr Tennison: Yes.

The Chair: I can see Anna Thomas chomping at the bit.

Anna Thomas: I would back up what Jeni is saying about group impacts in the workplace context. It is very important that individuals know how systems are used, why and where they have significant effects, and that risks and impacts are ascertained in advance. If it is just individuals and not groups or representatives, it may well not be possible to know, ascertain or respond to impacts in a way that will improve and maximise good outcomes for everybody—at an individual level and a firm level, as well as at a societal level.

I can give a few examples from work. Our research covers people being told about the rates that they should hit in order to keep their job, but not about the factors that are being taken into account. They are simply told that if you are not hitting that, you will lose your job. Another example is that customer interaction is often not taken into account, because it is not something that can be captured, broken down and assessed in an automated way by an algorithmic system. Similarly, older workers—they are very important at the moment, given that we need to fill vacancies and so on—are feeling that they are being "designed out".

Our research suggests that if we think about the risks and impacts in advance and we take proportionate and reasonable steps to address them, we will get better outcomes and we will get innovation, because innovation should be more than simply value extraction in the scenarios that I have set out. We will improve productivity as well. There is increasing evidence from machine learning experts, economists and organisational management that higher levels of involvement will result in better outcomes.

The Chair: Mr Birtwistle?

Michael Birtwistle: I very much agree with my other panellists on those points. If you are thinking about concrete ways to improve what is in the Bill, the high level of protection around automated decision making is currently in article 22B. That looks at decisions using special category data, which, as an input, you could also add in there, looking at the output. You could include decisions that involve high-risk processing, which is already terminology used throughout the Bill. That would mean that, where automated decision making is used around decisions that involve high-risk processing, you would need meaningful human involvement, explicit consent or substantial public interest.

Q73 Carol Monaghan: Jeni, can I come back to you on automated decision making? You have suggested that a requirement to notify people when an automated decision is made about them would be a useful inclusion in the Bill. Do you think enough consideration has been given to that?

Dr Tennison: The main thing that we have been arguing for is that it should be the wider set of decision subjects, rather than data subjects, who get rights relating to notification, or who can have a review. It is really important that there be notification of automated decision making, and as much transparency as possible about the details of it, and the process that an organisation has gone through in making an impact assessment of what that might mean for all individuals, groups and collective interests that might be affected by that automated decision making.

Q74 Carol Monaghan: We can probably broadly split these decisions into two categories. Decisions are already being made by algorithms online, according to what we are looking at. If I look up a paint colour online, and then start getting adverts for different paint companies, I am not too worried about that. I am more concerned that decisions could be made in the workplace about me, or about energy tariffs, as we have heard. That is more serious. Is there a danger that if we notify individuals of all the automated decisions that are made, it will end up like the cookie scenario—we will just ignore it all?

Dr Tennison: I do not think it is a matter of notifying people about all automated decision making. The Bill suggests limiting that to legally or otherwise significant decisions, so that we have those additional rights only as regards things that will really have an impact on people's lives.

Q75 Carol Monaghan: And you are not comfortable that those have been considered properly in the Bill.

Dr Tennison: I am not comfortable that they are directed to the right people.

Q76 Carol Monaghan: The subject, rather than the decision maker.

Dr Tennison: Yes.

Carol Monaghan: Anna, did you want to come in on that?

Anna Thomas: The last question about the threshold is really important, and it tends to suggest that work should have separate consideration, which is happening all over the world. Last week, Canada introduced its automated decision-making directive, and extended it to work. We have been working with it on that. Japan has a strategy that deals expressly with work. In the United States there are various examples, including the California Privacy Rights Act, of rules that give work special attention in this context. Our proposal for addressing the issue of threshold is that you should always provide notification, assess, and do your best to promote positive impacts and reduce negative ones if the decision-making impacts access to work, termination, pay, contractual status or terms, and, for the rest, when there is significant impact.

Q77 Carol Monaghan: Is there a danger that automated decisions could impact the Equality Act, if biases are not properly accounted for?

Anna Thomas: Yes, absolutely. In our model, we suggest that the impact assessment should incorporate not just the data protection elements, which we say remain essential, but equality of opportunity and disparity of outcome—for example, equal opportunity to promotion, or access to benefits. That should be incorporated in a model that forefronts and considers impacts on work.

Q78 Mike Amesbury: Anna, how would you strengthen the Bill? If you were to table an amendment around employees and AI, what would it be?

Anna Thomas: I would advise very clear additional rights, and a duty to notify in advance what, how and why AI is being used where it has these impacts, and where it meets the threshold that I was just asked about. I would also advise having more consultation throughout design, development and deployment, and ongoing monitoring, because AI changes, and there are impacts that we have not thought about or cannot ascertain in advance.

There should also be a separate obligation to conduct an algorithmic impact assessment. The Bill does nudge in that direction, but it says that there should be an assessment, rather than a data protection impact assessment. We suggest that the opportunity be grasped of clarifying that—at least in the workplace context, but arguably there are lessons more widely—the assessment ought to cover these fundamental aspects, and impacts at work.

Q79 Dr Huq: It is good to see the Ada Lovelace Institute represented; she was a pioneering woman computer scientist who lived in my constituency, so it is a bit ironic that the one man here is representing the institute.

Michael Birtwistle: My colleagues could not be here, unfortunately, but they would have been better representatives in that sense.

Dr Huq: I want to touch on the equality issue again. A 2019 UN report on the digital welfare state made the point that algorithms repeat existing biases and entrench inequalities. How do we get around that? There are a lot of issues around trust and people's rights and protections when it comes to this data. On top of those, there is this issue. Does the legislation address that? How can we overcome it?

Dr Tennison: As I have mentioned, there need to be more points in the Bill where explicit consideration of the public interest, including equality, is written into the sets of considerations that organisations, the ICO and the Secretary of State need to take into account when they are exercising their rights. That includes ensuring that public interest and equality are an explicit part of assessments of high-risk processing. That will help us to make sure that in the assessment process, organisations are made to look beyond the impacts on individuals and data subjects, and to look at the whole societal and economic impacts—even at the environmental impacts—that there might be from the processing that they are looking to carry out.

Anna Thomas: I agree. To add to what I said before, it would help to require a technical bias audit as well as a wider equality impact assessment. One idea that you may wish to consider is this: in the same way that the public sector has an obligation sometimes to consider the reduction of wider inequalities, you could have—well, not a full private sector model requiring that; that may need to be built up over time. We could, at the very least, require consideration of the desirability of reducing inequalities of opportunity and outcome as part of determining our reasonable and proportionate mitigations in the circumstances; that would be easy to do.

Michael Birtwistle: I agree. There is also a question about institutional capability—ensuring that the institutions involved have the capability to react to the use of these technologies as they evolve. Specifically, it would be great to see the ICO asked in the Bill to produce guidance on how the safeguards in article 22C are to be implemented, as that will have a large effect on how automated decision making will be lived in practice and built into firms. The powers reserved for Ministers around interpreting meaningful human involvement, and legal and similarly significant effect, will also have a big impact. It would make more sense for that to be with the ICO.

Dr Huq: Can I add one yes/no question?

The Chair: Yes.

Q80 Dr Huq: If we have an already overburdened regulatory framework, and we put AI on top of it, will it just fall through the cracks? Is there a danger that AI gets forgotten?

Michael Birtwistle: Yes, if regulators are not properly empowered.

Anna Thomas: I strongly agree, but they could be properly empowered and resourced, and in some instances given extra powers to interrogate or to redress what they have found. We advised that there should be a forum in 2020, and are delighted to see the Digital Regulation Cooperation Forum. That could be given additional resources and additional bite, and we would certainly like to see work forefronted and involved in activities. The forum would be well placed, for example, to provide dedicated cross-cutting guidance on impacts in work.

Dr Tennison: I agree with the other panellists. The only thing I would add is that I think that the involvement of the public will be absolutely essential for moving trust forward in those circumstances.

The Chair: The last question is from Chi Onwurah.

Q81 Chi Onwurah: Dr Tennison, could you give an example of the kind of abuse that you are most concerned about taking place if this Bill is passed unchanged, so that we can better understand your concern? And do I have time to ask—

The Chair: You have four minutes.

Chi Onwurah: Great. Ms Thomas, presumably all the automated decisions will be subject to employment law. Would employees have the information they need to appeal decisions and take them to an industrial tribunal?

Dr Tennison: You asked what kind of abuse I am particularly concerned about. I echo some of Anna's concerns around the work context and what that looks like. We have recently been doing some case studies, which again I can share, and they really bring home the kinds of issues that workers are subject to as automated decision making is rolled out in organisations.

More broadly, though, I am concerned about the gradual drift of reducing trust in the public sphere when it comes to the use of data by Governments and organisations. In some ways, I am more concerned about this leading to people not adopting technology and opting out of data collection because they are worried about what might happen. That would hold us back from the progress and the good uses of data that I would really like to see.

Michael Birtwistle: I agree with that very much. We need to think about past public concern around GP data sharing, contact tracing and the Ofqual exams algorithm. When people see their data being used in unexpected ways, or in ways that make them feel uncomfortable, they withdraw their consent and support for that use, and we as a society lose the benefits that data-driven technology can bring.

Anna Thomas: Employment law and the other laws in that context certainly help in some areas; for example, there is unfair dismissal protection, and redundancy protection under the information and consultation regulations. However, it is a patchwork, and it is not clear. Clarity is needed for businesses, to reassure people at work that the principles in the AI White Paper ultimately apply to their data, and to promote prosperity and wellbeing as widely as possible.

The Chair: I thank our three witnesses very much indeed; you have all been fantastic. We are very grateful to you for being here. That brings us to the end of our morning session. The Committee will meet again at 2 o'clock, here in the Boothroyd Room, to continue taking oral evidence. We heard from 10 witnesses this morning and will hear from 13 this afternoon.

Ordered, That further consideration be now adjourned. *—(Steve Double.)*

11.23 am

Adjourned till this day at Two o'clock.

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Second Sitting

Wednesday 10 May 2023

(Afternoon)

CONTENTS

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

Sunday 14 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
† Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Eastwood, Mark *(Dewsbury)* (Con)
Henry, Darren *(Broxtowe)* (Con)
Hunt, Jane *(Loughborough)* (Con)
† Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Monaghan, Carol *(Glasgow North West)* (SNP)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
† Richards, Nicola *(West Bromwich East)* (Con)
Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Witnesses

Tom Schumacher, Chief Privacy Officer, Medtronic

Jonathan Sellors MBE, Legal Counsel and Company Secretary, UK Biobank

Harry Weber-Brown, Chief Engagement Officer, ZILO

Phillip Mind, Director, Digital Technology and Innovation, UK Finance

Keith Rosser, Chair, Better Hiring Institute

Helen Hitching, Deputy Director and Chief Data Officer, National Crime Agency

Aimee Reed, Director of Data, Metropolitan Police

Andrew Pakes, Director of Communications and Research, Prospect

Mary Towers, Policy Officer, TUC

Alexandra Sinclair, Research Fellow, Public Law Project

Ms Laura Irvine, convener of the Privacy Law sub-committee, Law Society of Scotland

Jacob Smith, UK Accountability Team Leader, Rights and Security International

Alex Lawrence-Archer, Solicitor for AWO (a data rights agency)

Public Bill Committee

Wednesday 10 May 2023

(Afternoon)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

Examination of Witnesses

Tom Schumacher and Jonathan Sellors gave evidence.

2 pm

The Chair: Welcome back. We are now on to our fifth witness panel and we will hear from Tom Schumacher, chief privacy officer at Medtronic, who has kindly joined via Zoom, and Jonathan Sellors, legal counsel and company secretary at UK Biobank, who is in the room. We have until 2.25 pm for this panel. Could the witnesses please introduce themselves for the record?

Jonathan Sellors: Good afternoon. I am Jonathan Sellors, general counsel of UK Biobank. To those who may not know, we are the largest globally accessible clinical research resource in the world. We comprise 500,000 UK-based participants, and we make de-identified data available to researchers to conduct clinical research in the public interest.

Tom Schumacher: Thank you so much for inviting me. I am Tom Schumacher, and I work for Medtronic as the chief data and privacy counsel. Medtronic is the world's largest medical device maker, with 90,000 employees around the world and three manufacturing sites in the UK. We are headquartered in Ireland.

The Chair: Thank you both for joining us. Stephanie Peacock.

Q82 Stephanie Peacock (Barnsley East) (Lab): Welcome to you both. My first question is to both witnesses. How easy is it currently for service users and care teams to access and share all of their relevant health and care data?

Jonathan Sellors: I am not sure I am the expert on this particular topic, because my experience is more research-based than in IT systems embedded in clinical care.

Tom Schumacher: I am also not as intimately familiar with that issue, but I would say that interoperability is absolutely critical. One of the challenges we experience with our technologies—I assume this is also the case for your health providers—is the ability to have high-quality data that means the same thing in different systems. That is a challenge that will be improved, but it is really a data challenge more than a privacy challenge. That is how I see it.

Q83 Stephanie Peacock: Will the new definition in the Bill of what constitutes scientific research help people in your field to conduct more or better research? If so, what impact would this research have on citizens and healthcare?

Jonathan Sellors: I think it is a thoroughly useful clarification of what constitutes research. It is essentially welcome, because it was not entirely clear under the provisions of the General Data Protection Regulation what the parameters of research were, so this is a helpful clarification.

Tom Schumacher: I completely concur: it is very useful. I would say that a couple of things really stand out. One is that it makes it clear that private industry and other companies can participate in research. That is really important, particularly for a company like Medtronic because, in order to bring our products through to help patients, we need to conduct research, have real-world data and be able to present that to regulators for approval. It will be extremely helpful to have that broader definition.

The other component of the definition that is quite helpful is that it makes it explicit that technology development and other applied research constitutes research. I know there is a lot of administrative churn trying to figure out what constitutes research and what does not, and I think this is a really helpful piece of clarification.

Q84 The Minister for Data and Digital Infrastructure (Sir John Whittingdale): Perhaps I could ask you both to elaborate on how the existing definition and the current lack of clarity have impeded you in carrying out the research you would like to do and how this will change as a result of the Bill.

Tom Schumacher: Maybe I can give an example. One of the businesses we purchased is a business based in the UK called Digital Surgery. It uses inter-body videos to try to improve the surgery process and create technologies to aid surgeons in prevention and care. One of the challenges has been, to what extent is the use of surgery videos to create artificial intelligence and a better outcome for patient research? Ultimately, it was often the case that a particular site or hospital would agree, but it created a lot of churn, activity and work back and forth to explain exactly what was to be done. I think this will make it much clearer and easier for a hospital to say, "We understand this is an appropriate research use" and to be in a position to share that data according to all the protections that the GDPR provides around securing and de-identifying the data and so on.

Jonathan Sellors: I think our access test, which we apply to all our 35,000 users, is to ensure they are bona fide researchers conducting health-related research in the public interest. We quite often get asked whether the research they are planning to conduct is legitimate research. For example, a lot of genetic research, rather than being based on a particular hypothesis, is hypothesis-generating—they look at the data first and then decide what they want to investigate. This definition definitely helps clear up quite a few—not major, but minor—confusions that we have. They arise quite regularly, so I think it is a thoroughly helpful development to be able to point to something with this sort of clarity.

Q85 Sir John Whittingdale: Can you say a little about the extent to which you have been a contributor to the design of the new provisions in the Bill and whether you are happy with the outcome of that?

Jonathan Sellors: The short answer would be yes. I was contacted by NHS England about the wording of some of the consent aspects, some of the research aspects and particularly some of the pseudonymisation

aspects, because that is an important wall. Most research conducted is essentially on pseudonymised rather than identifiable data. The way it has been worded and clarified, because it makes an incremental improvement on what is already there in the GDPR, is very useful. I think it is a good job.

Tom Schumacher: Yes, I would say the same. NHS Transformation and the Department for Culture, Media and Sport, particularly Owen Rowland and Elisabeth Stafford, have been very willing to hear points of view from industry and very proactive in reaching out for our feedback. I feel like the result reflects that good co-ordination.

Q86 Damian Collins (Folkestone and Hythe) (Con): Do you think the definition of what public health means in the context of the Bill is clear?

Jonathan Sellors: Yes, I think it is reasonably clear.

Damian Collins: What do you mean by that?

Jonathan Sellors: Like any lawyer, if I were asked to draft something, I would probably always look at it and say I could possibly improve it. However, I would actually look at this and say it is probably good enough.

Q87 Damian Collins: What do you think it means? What is the scope of it?

Jonathan Sellors: If I may, can I come back to you on that with a written response, when I have given it slightly further consideration? Would that be okay?

Q88 Damian Collins: Yes. What I would be interested in is that there could be medical research linked to physical ailments. It could also include mental health, which could, in this context, open up quite a wide range of different fields of research for commercial application as well—understanding people's stimulus response to fear, anxiety and so on, some of which could have medical application and some of which could be purely commercial.

Jonathan Sellors: I think that, with health-related research that is in the public interest, it is relatively straightforward to spot what it is. Most research is going to have some commercial application because most of the pharma, molecules and medical devices are going to be commercially devised and developed. I do not think that the fact that something has a commercial interest should count it out in any way; it is just about looking at what the predominant interest is.

Q89 Damian Collins: I think that is right. I would welcome it if you were able to write to the Committee with some further thoughts on that. My point, I suppose, is that we have a pretty good idea of what we think public health research could be in this context, whether it is for commercial or non-commercial reasons. However, we want to be certain about whether that opens up other channels of research that others may regard as being not about solving public health problems, but just about the commercial exploitation of data.

Jonathan Sellors: Right, thank you. I understand.

Tom Schumacher: I concur with what the previous speaker said. In the medical device industry, we really focus on what is considered more traditional research, which fits well within the refined research definition that the Bill contains.

Q90 Damian Collins: I have a final question. We have this legislation, and then different tech companies and operating systems have separate guidelines that they work to as well. One of the issues the Government faced with, for instance, the covid vaccine app, was that it had to comply with the operating rules for Google and iOS, regardless of what the Government wanted it to do. Thinking of the work that your organisation has been involved in, are there still significant restrictions that go beyond the legal thresholds because different operating systems set different requirements?

Jonathan Sellors: I do not think I am really the best qualified person to talk about the different Android and Apple operating systems, although we did a lot of covid-related work during the pandemic, which we were not restricted from doing.

Tom Schumacher: I would say that this comes up quite a lot for Medtronic in the broader medtech industry. I would say a couple of things. First, this is an implementation issue more than a Bill issue, but the harmonisation of technical standards is absolutely critical. One of the challenges that we, and I am sure NHS trusts, experience is variability in technical and IT security standards. One of the real opportunities to streamline is to harmonise those standards, so that each trust does not have to decide for itself which international standard to use and which local standard to use.

I would also say that there is a lot of work globally to try to reach international standards, and the more that there can be consistency in standards, the less bureaucracy there will be and the better the protection will be, particularly for medical device companies. We need to build those standards into our product portfolio and design requirements and have them approved by notified bodies, so it is important that the UK does not create a new and different set of standards but participates in setting great international standards.

Q91 Rebecca Long Bailey (Salford and Eccles) (Lab): In relation to medical research, concerns have been raised that the Bill might risk a divergence from current EU adequacy and that that might have quite a significant detrimental impact on collaboration, which often happens across the EU on medical research. Are you concerned about that, and what should the Government do to mitigate it?

Jonathan Sellors: I think that it is absolutely right to be concerned about whether there will be issues with adequacy, but my evaluation, and all the analysis that I have read from third parties, particularly some third-party lawyers, suggests that the Bill does not or should not have any impact on the adequacy decision at all—broadly because it takes the sensible approach of taking the existing GDPR and then making incremental explanations of what certain things actually mean. There are various provisions of GDPR—for example, on genetic data and pseudonymisation—that are there in just one sentence. It is quite a complicated topic, so having clarification is thoroughly useful, and I do not think that that should have any impact on the adequacy side of it. I think it is a very important point.

Tom Schumacher: I agree that it is a critical point. I also feel as though the real value here is in clarifying what is already permitted in the European GDPR but doing it in a way that preserves adequacy, streamlines and makes it easier for all stakeholders to reach a quick

and accurate decision. I think that adequacy will be critical. I just do not think that the language of the text today impacts the ability of it to be adequate.

Q92 Chi Onwurah (Newcastle upon Tyne Central) (Lab): I know that you are very supportive of the Bill, but I wonder whether you see risks to patients and service users from facilitating a greater sharing of health and care data. Could you each answer that question?

Jonathan Sellors: I think that data sharing, of one sort or another, absolutely underpins medical research. You need to be able to do it internationally as well; it is not purely a UK-centric activity. The key is in making sure that the data that you are using is properly de-identified, so that research can be conducted on patients, participants and resources in a way that does not then link back to their health data and other data.

Q93 Chi Onwurah: So it has to be de-identified. We will return to that. But you do not see any other risks?

Jonathan Sellors: Let me put it this way: poor-quality research, undertaken in an unfortunate way, is always going to be a problem, but good-quality research, which has proper ethical approval and which is done on data that is suitably managed and collated, is an essential thing to be able to do.

Q94 Chi Onwurah: I agree with you. Sorry, I did not quite hear what you said—approval by whom?

Jonathan Sellors: Approval by the relevant ethics committee.

Q95 Chi Onwurah: Right. Is it a requirement of the Bill that the research should have the approval of the relevant ethics committee?

Jonathan Sellors: I do not think that it is a requirement of this Bill, but it is a requirement of pretty much most research that takes place in the UK.

Q96 Chi Onwurah: But not all research, surely, because the definition of research is something that can

"reasonably be described as scientific"

research. You would see concerns, then, if data was to be shared for research that was carried out outside of ethics committee approvals. I do not want to put words into your mouth, but I am just trying to understand.

Jonathan Sellors: Sure. I think it depends on the nature of the data that you are trying to evaluate. In other words, if you are looking at aggregated or summary datasets, I do not think there is any particular issue, but when you are looking at individual-level data, that has to be suitably de-identified in order for research to be safely conducted.

Q97 Chi Onwurah: On the point of de-identifying or pseudonymisation, do you recognise that there have been examples of pseudonymised data that has been re-identified, and that, particularly given the rise of huge datasets, artificial intelligence and so on, there is a risk of un-de-identifying pseudonymised data?

Jonathan Sellors: There is always a risk, but I think the way it is expressed in the Bill is actually quite measured. In other words, it takes a reasonable approach to what steps can constitute re-identification. There are a certain police-related examples whereby samples are found on crime scenes. The individuals can be identified, certainly, if you are on the police database, but if they are not on a reference database, it is extremely difficult to re-identify them, other than with millions of pounds-worth of police work. For all practical purposes, it is actually de-identified. Saying something is completely de-identified is quite difficult.

Q98 Chi Onwurah: Yes, I certainly agree with that—it is almost impossible—but I do think it is possible to re-identify data without spending millions of pounds, especially when it is correlated with other large datasets. Would you recognise that?

Jonathan Sellors: I definitely recognise that. That is one of our principal bits of concern, but usually the identifiers are the relatively simple ones. In other words, you can re-identify me quite easily by my seven-digit postcode and my age and my gender. Obviously, when we release data, we make sure not to do that. Releasing quite a big bit of my genetic sequence does not make me re-identifiable.

Chi Onwurah: Currently.

Jonathan Sellors: Currently—I accept that.

Tom Schumacher: I would say a couple of things. It is important to know that the Bill preserves the full array of safeguards in the GDPR around data minimisation, access controls and making sure that you have de-identified the data as much as possible for the purpose you are going to use it for. The opportunity that our company is quite concerned about is that, without some elements of real-world data, we are not going to be able to eliminate the bias that we see in the system. We are not going to be able to personalise medicine, and we are not going to be able to get our products approved, because our regulating bodies are now looking at and mandating that the technology we use is tested in different attributes that are relevant for that technology.

As an example, there are very few data pieces that we need for our digital surgery business, but we might need gender, weight and age. The Bill will allow customisation to say, "Okay, what are you going to do to make sure that only two or three data scientists see that data? How are you going to house it in a secure, separate environment? How are you going to make sure that you have security controls around that?" I think the Bill allows that flexibility to try to create personalised medicine, but I do not believe that the Bill opens up a new area of risk for re-identification provided that the GDPR safeguards remain.

Q99 Chi Onwurah: Let me ask a follow-up question. I recognise that your intent in research is ethical—there are ethics committees involved. Given the definition of scientific research to be anything that can be reasonably described as scientific, what is to stop data being shared for the purposes of, for example, justifying anti-covid vaccination conspiracy theories? Do you recognise that there are purposes that could be described as research but which many people would not want their data to be used for?

Tom Schumacher: In isolation, that would be a risk, but in the full context of the interrelationship between the data owner and controller and the manufacturer, there would be a process by which you would define the

legitimate use you are going to use that data for, and that would be something that you would document and would go on your system. I do not believe that using data for political purposes would constitute research in the way that you would think about it in this Bill. Certainly the UK ICO is well regarded for providing useful interpretation guidance. I think that that office would be able to issue appropriate guardrails to limit those sorts of abuses.

Jonathan Sellors: If you look at a scientific hypothesis, it might not be a scientific hypothesis that you like, but it is much better to have it out there in the public domain, where the data that underpins the research can be evaluated by everybody else to show that it is not sound and is not being conducted appropriately.

Q100 Chi Onwurah: Yes, but people might not want their data to be used for that. They would have no control over it in this case.

Jonathan Sellors: There has to be some element of scientific flexibility, but scientists themselves have to be able to make a decision about what they wish to investigate. The main thing to ensure is that it is transparent—in other words, somebody else can see what they have done and the way in which they have done it, so that if it does come up with a conclusion that is fundamentally flawed, that can be properly challenged.

The Chair: If there are no further questions, may I thank both of you gentlemen very much indeed for your time this afternoon and for giving us your evidence. It is hugely appreciated. We now move on to the sixth panel.

Examination of Witnesses

Harry Weber-Brown and Phillip Mind gave evidence.

2.23 pm

The Chair: Welcome, gentlemen. We will now hear from Harry Weber-Brown, chief engagement officer at ZILO, and Phillip Mind, director of digital technology and innovation at UK Finance. We have until 2.50pm for this session. I now invite the witnesses to please introduce themselves to the Committee for the record, starting with Mr Weber-Brown.

Harry Weber-Brown: Thank you very much. My name is Harry Weber-Brown, chief engagement officer for ZILO Technology Ltd, which is a start-up based in London. I have previously worked for the Investing and Saving Alliance. I have much experience in both smart data, which is dealt with in part 3 of the Bill, and digital identity, which relates to digital verification services in part 2.

Phillip Mind: Good afternoon. I am Phillip Mind, director of digital technology and innovation at UK Finance, a trade body representing over 300 organisations in the bank and finance community. Like Harry, my expertise resides more in parts 2 and 3 of the Bill, although I have a few insights into part 1.

Q101 Stephanie Peacock: Good afternoon to both witnesses. I have a broad opening question. What are the main implications of the Bill's provisions for the finance sector?

Phillip Mind: The banking community is supportive of the Bill, which is enabling of a digital economy. The data protection reforms reduce compliance burdens on business, which is very welcome. The provisions on digital identity are enabling, and we see digital identity as an essential utility for customers in the future. The provisions on smart data extend an open data regime to other sectors. We already have an open banking regime, and we are keen for that to extend to other sectors. It offers real opportunities in terms of innovative products and services, but we would caution the Committee that there is significant cost and complexity in those measures.

Harry Weber-Brown: The Bill is key to retaining the UK's place as a hub for technical innovation, and in particular for investment in fintech. It is critical also to make sure the UK remains a global leader in data portability. Building on the work that Phillip just mentioned on open banking, which has over 7 million users among both consumers and small and medium-sized enterprises, it is critical that we make sure we are ahead of the competition.

For the financial services sector, the provisions on ID help to reduce costs for things like onboarding and reduce fraud for things like authorised push payments. It also delivers a better customer experience, so you do not have to rummage around to find your passport every time you want to set up a new account or need to verify yourself to a financial service firm.

Smart data is an opportunity for us to extend ourselves as the world leader in open finance, building on the work of not only open banking but the pensions dashboard, which is yet to be launched but is another open finance scheme. The opportunity to widen up and give consumers more control in their ability to share data is critical for the customer, the economy and the financial services industry.

Q102 Stephanie Peacock: That is great. You both mentioned smart data. For the benefit of the Committee, could you outline some of the progress that the banking and finance industries have made in developing smart data initiatives?

Phillip Mind: In the banking industry we have open banking, which allows customers to choose and consent to allow an authorised third party provider access to their account to provide products and services—access to see the data. It also allows—again, with customer choice and consent—customers to allow a third party provider to make payments on their behalf. That has been hugely enabling. It has enabled growth in all sorts of innovative products and services and growth in fintech in the UK. As Harry mentioned, there are over 7 million active customers at the moment, but it does come with a cost; it is not a free good. Making that service available has involved cost and complexity.

In extending the provisions to other sectors through secondary legislation, it is really important that we are cognisant of the impacts and the unintended consequences. Many sectors have pre-existing data-sharing arrangements, many of which are commercial, and it is important that we understand the relative costs and benefits and how they fall among different participants in the market. My caution to the Committee and to Government is to go into those smart data schemes with eyes open.

Q103 Stephanie Peacock: To develop that point, do you think there are enough safeguards in the Bill to ensure that Ministers assess the commercial sense and the impact of any new smart data regimes before regulating for them?

Phillip Mind: Clauses 62 and 64 make provision for the Secretary of State and Treasury to consult on smart data schemes. We think that those provisions could be strengthened. We see a need for impact assessments, cost-benefit analysis and full consultation. The Bill already allows for a post-implementation review, and we would advise that too.

Harry Weber-Brown: I think the other one to call out is the pensions dashboard, which has been driven out of the Money and Pensions Service. Although it has not actually launched yet, it has brought the life assurance industry on the site to develop free access to information. The consumer can see all their pensions holdings in a single place, which will then help them to make better financial decisions.

I think my former employer, the Investing and Saving Alliance, was working on an open savings, investments and pensions scheme. Obviously, that is not mandatory, but this is where the provision for secondary legislation is absolutely imperative to ensure that you get a wide scope of firms utilising this. At the moment, it is optional, but firms are still lining up and wanting to use it. There is a commitment within the financial services industry to do this, but having the legislation in place—secondary legislation, in particular—will ensure that they all do it to the same standards, both technical and data, and have a trust framework that wraps around it. That is why it is so imperative to have smart data.

Q104 Sir John Whittingdale: Would you say a little about the international position? You referred to the UK's position as a leader in this field. To what extent is that the case? What are the benefits, and what is the risk to the UK's position if we do not make the changes proposed in the Bill?

Harry Weber-Brown: In part 2 or part 3 of the Bill? The digital verification services or smart data?

Sir John Whittingdale: I will come on to digital verification. Let us focus on smart data, to begin with.

Harry Weber-Brown: On that, Australia is certainly one of the leaders. The consumer has a data right under legislation that enables them to recall information from across a variety of sectors, not just financial services, and to have their information in a structured format shared with a data consumer—a third-party provider in open banking. Things are afoot. A lot of work is going on in the States, but less in Europe, interestingly. Legislation is coming through, but I think the big country to watch from our perspective is Australia and what has happened there. Theirs is a more far-reaching approach than, say, we have. That is for the smart data side.

There is a risk that if we do not extend that data right to other financial services, the consumer has a very limited view of what they can actually share. They can share their bank account details and possibly their pensions data as well, but what about their savings and investments, certainly in non-pension type wrappers? Give the consumer a full, holistic view of all their holdings and their debt as well, so that they can see their balance, as it were, and make better financial decisions. That is why we think it is so important to have part 3 of the Bill go through and for secondary legislation to follow behind it.

There is a risk that if we do not do that, the consumer has a very fragmented view. Does that mean that overseas, where it is legislated for, the consumer would have a more holistic view of everything? Would that drive investment overseas, rather than into the UK? As Phillip said, open banking has really heralded a range of fintech providers being able to consume data and provide value-added services on top of that banking data. I think it rebalances the marketplace as well.

Phillip Mind: To build on Harry's remarks, I think that the real opportunity is for the UK to build a flourishing fintech industry. We have that already; open banking is actually one of our exports. Our way of doing open banking—the standards and the trust framework—has been a successful export, and it has been deployed in other jurisdictions. The opportunity around open data is to maintain that competitiveness for UK fintech when it is trading abroad.

Most of the consequences of extending beyond open banking into other smart data schemes impact UK businesses and consumers. I do not necessarily see that there is a competitiveness issue; it is bounded within the domestic economy.

Q105 Sir John Whittingdale: Moving on to the digital identity provisions, clearly some people are already familiar with this, but there is still a degree of suspicion. To what extent do you think that the consumer needs persuasion about the security and the benefits of digital identity services? Do you see that as being addressed by the provisions in the Bill?

Harry Weber-Brown: That is a very good question. I did quite a lot of consumer research in my previous capacity, and consumers are initially quite sceptical, asking "Why are you asking me for identity details and things?" You have to explain fully why you are doing that. Certainly having Government support and things like the trust framework and a certification regime to make sure that the consumer knows whom they are dealing with when they are passing over sensitive data will help to build the trust to ensure that consumers will utilise this.

The second part to that is what types of services are built on top of the identity system. If I have the identity verified to an AML—anti-money laundering—standard for financial services, I could use it for a whole suite of other types of activity. That could be the purchase of age-restricted products, or sharing data with my independent financial adviser; it could reduce fraud in push payments, and so on. There is a whole suite of different types of services; you would not be using it just for onboarding. I think the Government support of this under digital verification services, part 2 of the Bill, is critical to make sure it happens.

It is opt-in. We are not saying to people that they have to get an identity card, which obviously is not hugely popular; but if we can demonstrate the value of having a digital identity, with support and trust—with the trust framework and certification with Government—we will not necessarily need to run a full marketing campaign to make sure that consumers use this.

Look at other territories—for example, Norway with Vipps, or Sweden's BankID. I think about 98% of the population now use ID in a digital format; it is very commonplace. It is really a question of looking at the use cases—examples of how the consumer could utilise this—and making sure they receive utility and value from the setting up and the utilisation of the ID. The ID by itself is not necessarily compelling enough; the point is what you can use it for.

Phillip Mind: Trust and acceptance are key issues, and the Bill lays the legislative foundations for that. We already assert our identity digitally when we open accounts, but we do so on a one-off basis. The challenge is to go from doing so on a one-off basis to creating a digital token that is safe and secure and that allows us to reuse that digital identity. For that to work, that token has to be widely accepted, and that is a really complex strategic challenge, but the Bill lays the foundations.

We will transact digitally more and more; that is for sure. At the moment, we have a consultation, from the Treasury and the Bank of England, on a central bank digital currency. Arguably, that would benefit hugely from a reusable digital identity, but we need to be able to create the token in the right way. It could be enabling for people who have access to a smartphone but do not have a passport or driving licence; it could also build inclusion, in terms of identity. So we are very supportive of a reusable digital identity, but it is a big challenge, and the challenge is gaining trust and acceptance.

Q106 Damian Collins: Mr Weber-Brown, you in particular have spoken about the consumer benefits of data sharing—having a wider choice of products and services. What do you see as the principal business benefits for financial service providers? How wide would you like the scope of their access to data to be?

Harry Weber-Brown: Financial services obviously rely heavily on data to be able to fashion their products accordingly and make them personal, so I think it is critical to have a smart data regime where everything is collected in a single format—what is known as an API, an application programming interface, which is a common way of securely sharing data.

Some of the other use cases from smart data that would benefit business would be things like sharing data around fact find. For example, if someone wants to instruct an independent financial adviser, could they not use this as a way of speeding up the process, rather than having to wait on letters of authority, which are written and take time? Similarly, with pension providers, if I wanted to move from one pension to another or to consolidate things, could we use the smart data to get an illustration of what impact that might have, so that before I ported it over I could see that?

For big financial services firms—well, for all of them—efficiencies are delivered because, as my colleague said, we are using digital as opposed to having to rely on manual processing. As long as the safeguards are put in place, that spawns a whole array of different types of use case, such as with regulatory reporting. If I need to report things to the regulator, could I use smart data provision to do that? That would benefit businesses. A lot of the financial services industry still relies on reporting on Excel spreadsheets and CSV files, so if we can digitise that, it would certainly make it a much more efficient economy.

Q107 Damian Collins: Can you understand that there might also be concerns on the consumer side about data profiling consumers based on risk? That would make a lot of sense for financial services. You have described certain financial products, but equally there are people offering loans, mortgages, insurance and things like that who will be very keen to understand more about their customers before pricing their products accordingly.

Phillip Mind: A digital identity gives customers more control. One of the issues that we face at the moment when we present a passport or driving licence is that we cannot minimise the data there. There is a data minimisation opportunity and benefit.

For businesses and customers, too, identity is a key issue when we transact digitally. There are risks around profiling, but there are real opportunities around anti-fraud as well. Being absolutely clear about who we are transacting with and being able to prove incontrovertibly who we are through a safe and secure token will deliver huge benefits to the economy.

Damian Collins: We talked in the previous session about the undoubted benefits, which you have set out clearly. Equally, however, consumers will still want to know what sort of data about them is being used and who has access to it. For example, if a video games maker is profiling the attitudes of players to risk, in order to stimulate them with risk-and-reward opportunities within a game like Fortnite, consumers might understand how that makes their gameplay more interesting. They might consent to that, but they might not necessarily want a financial services provider to have access to that information, because it could create a picture of them that is not flattering.

Harry Weber-Brown: That is a perfectly good challenge. There is a spawning part of the industry around consent dashboards. The idea there is that we put much more control in the hands of the consumer, so that they can see where they have given consent to share data and what data has been shared, while also having the right of revocation and so on. There are technical workarounds to ensure that consumers are much more empowered to control their data. Certainly the legislation supports that, but there will be the technical implementation that sits behind it to ensure that the GDPR is abided by and that the smart data will facilitate better services to consumers. The technology is the answer, but the smart data will open up the opportunity to make sure that the consumer is protected, while with things like consent dashboards they can take better control of where their data is being shared.

Phillip Mind: The interesting thing about digital identity is that it creates a tether. In the future, you will be able to tether digitalised tokens such as securities or deeds to an identity in a safe way, but you could also tether consent to a digital identity, giving a customer or citizen a more holistic view of what they have consented to and where. As Harry says, for those who have real data literacy issues, we will see intermediaries offering services around consent. Those services exist in other jurisdictions.

Damian Collins: I think the Estonian digital ID model works in a very similar way.

Q108 Chi Onwurah: You have both spoken very passionately, if I may say so, about the importance of citizens being in control of their data, particularly with

[Chi Onwurah]

open banking. We all take very seriously our financial data and the importance of trust and empowerment in these services. Can you say how the Bill will improve trust and control for citizens, or how it should do so?

Harry Weber-Brown: Part 2 of the Bill sets out the trust framework, which was being developed by the then Department for Digital, Culture, Media and Sport and which now comes under the Department for Science, Innovation and Technology. It will give certainty to the marketplace that any firm that wishes to store data—what is commonly known as an identity provider—will have to go through a certification regime. It will have to be certified against a register, which means that as a consumer I will know that I can trust that organisation because it will be following the trust framework and the policies that sit within it. That is critical.

Similarly, if we are setting up schemes with smart data we will need to make sure that the consumer is protected. That will come through in secondary legislation and the devil will be in the detail of the policies underpinning it, in a similar way to open banking and the pensions dashboard.

Further to the previous session, the other thing I would say is that we are talking on behalf of financial services, but parts 2 and 3 of the Bill also refer to other sectors: they apply equally to health, education and so on. If as a consumer I want to take more control of my data, I will want to be able to use it across multiple services and get a much more holistic view not just of my finances, but of my health information and so on.

One area that is particularly developing at the moment is the concept of self-sovereign identity, which enables me as a consumer to control my identity and take the identity provider out of the equation. I do not want to get too technical, but it involves storing my information on a blockchain and sharing my data credentials only when I need to do so—obviously it follows data minimisation. There are evolving schemes that we need to ensure the Bill caters for.

Q109 Chi Onwurah: Thank you very much for those points.

You mentioned data verification services. Briefly, can you help the Committee to understand who would be providing those services and who would be paying for them? You gave the example of tethering my property or other ownership. Who would be paying in that case? Would I be paying for the rest of my life to keep that data where it is? How do you see it working?

Phillip Mind: Who will provide the services? There is already a growing list of verified providers. There is a current market in one-off digital identity services, and I think many of those providers would step in to the reusable digital identity market.

What is the commercial model? That is a really good question, and frankly at this point I do not have an answer. That will evolve, but within the frameworks that are set up—trust schemes, in the jargon—there will be those who provide digital identity services and those organisations that consume them, which could be retailers, financial services providers or banks. It is likely that the relying parties, the consumers, would pay the providers.

Harry Weber-Brown: But not the individual consumers. If you wanted to open a bank account, and the bank was relying on identity measures provided by fintech, the bank would pay the fintech to undertake those services.

The Chair: We have time for a very quick question from Rupa Huq, with very quick answers.

Q110 Dr Rupa Huq (Ealing Central and Acton) (Lab): UK Finance's members are all the big banks—is that right?

Phillip Mind: We represent more than 300 organisations in the banking and finance community. Some are big banks and some are quite small fintechs, so there is quite a spectrum.

Q111 Dr Huq: Okay. The dealings that I have had with you have been about the bank card phenomenon. We know that there is public mistrust in the consumer banking sector about how our data is controlled. How will you ensure that the Bill does not leave behind those people who are not online? That is what the banking hubs are aimed at, is it not? There is a whole loneliness agenda, as well as issues relating to the elderly.

The Chair: You have 30 seconds to answer.

Phillip Mind: That is a big challenge. It is really important that people are not left behind and that they have the ability to create a kind of digital identity. As a society, we will have to work very hard to enable that. That is a responsibility that falls not on banks, but on other organisations that will help citizens to create these identities.

The Chair: Thank you very much indeed for your evidence this afternoon and for giving us the benefit of your time. We appreciate it.

Examination of Witness

Keith Rosser gave evidence.

2.50 pm

The Chair: Welcome, Mr Rosser. We have just 15 minutes, until 3.05 pm, for this session. Would you kindly introduce yourself to the Committee for the record?

Keith Rosser: My name is Keith Rosser. I am the chair of the Better Hiring Institute.

Q112 Stephanie Peacock: Good afternoon. What are the main implications of the Bill for employers? Specifically, how will enabling greater use of a digital verification service help employers to make hiring decisions?

Keith Rosser: Employers have been making hiring decisions using digital identity since 1 October, so we are a live case study. The biggest impact so far has been on the speed at which employers are able to hire staff and on the disconnection between where people live and the location of their job. For example, people in a digital identity scheme could apply for work, get a job and validate who they are without ever necessarily having to go and meet the employer. It is really important across the regions, from St Austell to Glasgow, that we

are opening up job opportunities across the UK, including in some of our urban areas—West Bromwich, Barnsley and others—where people get greater job opportunities from where they live because they are not tied to where the employer is. It has had a profound effect already.

We recently looked at a study of 70,000 hires or people going through a hiring process, and 83%—some 58,000—opted to take the digital identity route. They did it in an average time of three minutes and 30 seconds. If we compare that with having to meet an employer and go through a process to provide your physical documents, there is a saving of around a week. If we think about making UK hiring the fastest globally, which is our ambition, people can start work a week earlier and pay taxes earlier, and we are cutting waiting lists and workloads. There is a huge positive impact.

In terms of employers making those hiring decisions, technology is so much better than people at identifying whether a document is genuine and the person is who they say they are. In that case study, we found that 200 of the 70,000 people going through the process had fake documents or fraudulently obtained genuine documents. The question is, would the human eye have spotted that prior to the implementation of digital identity? I am certain that it would not have done. Digital identity is really driving the potential for UK hiring to be a shining example globally.

Q113 Stephanie Peacock: Do you think the provisions in the Bill will help to improve public trust in digital identities?

Keith Rosser: From that 70,000 example, we have not seen evidence yet that public trust has been negatively impacted. There are some very important provisions in the Bill that have to go a long way to assuring that. One is the creation of a governance body, which we think is hugely important. There has to be a monitoring of standards within the market. It also introduces the idea of certifying companies in the market. That is key, because in this market right now 30% of DVSs—nearly one in three companies—are not certified. The provision to introduce certification is another big, important move forward.

We also found, through a survey, that we had about 25% fewer objections when a user, company or employer was working with a certified company. Those are two really important points. In terms of the provision on improving the fraud response, we think there is a real opportunity to improve what DVSs do to tackle fraud, which I will probably talk about later.

Q114 Sir John Whittingdale: Perhaps I could ask you to expand on that now. To what extent would you say that some providers that are not certified are not meeting the standards necessary, or in some cases even promoting fraud?

Keith Rosser: I have every reason to believe that organisations not certified will not be meeting anywhere near the standards that they should be meeting under a certified scheme. That appears really clear. They certainly will not be doing as much as they need to do to tackle fraud.

My caveat here is that across the entire market, even the certified market, I think that there is a real need for us to do more to make sure that those companies are doing far more to tackle fraud, share data and work with Government. I would say that uncertified is a greater risk, certainly, but even with certified companies we must do more to make sure that they are pushed to meet the highest possible standards.

Q115 Sir John Whittingdale: So would you expect that as a result of the Bill, the bar to obtain certification will be higher?

Keith Rosser: Yes. The requirement on DVSs to tackle fraud should be higher than it currently is.

Q116 Damian Collins: I want to follow on from the Minister's questions. Looking at other legislation that is going through Parliament, particularly the anti-fraud provisions in the Online Safety Bill, one of the important areas is the extent to which regulators should expect companies to have good upstream solutions in place to combat fraud. Rather than chasing every example that they come across, they need things that block it in the first place. Do you see the provisions in this Bill as being helpful? Would you expect regulators to act on that and to direct companies to use systems that are known to be safe?

Keith Rosser: Absolutely. I will give a quick example relating to the Online Safety Bill and hiring, which I am talking about. If you look at people getting work online by applying through job boards or platforms, that is an uncertified, unregulated space. Ofcom recently did research, ahead of the Online Safety Bill, that found that 30% of UK adults have experienced employment scams when applying for work online, which has a major impact on access to and participation in the labour market, for many reasons.

Turning the question the other way around, we can also use that example to show that where we do have uncertified spaces, the risks are huge, and we are seeing the evidence of that. Specifically, yes, I would expect the governance body or the certification regime, or both, to really put a requirement on DVSs to do all the things you said—to have better upstream processes and better technology.

Also, I think there is a big missing space, given that we have been live with this in hiring for eight months, to provide better information to the public. At the moment, if I am a member of the public applying for a job and I need to use my digital identity, there is no information for me to look at, unless the employer—the end user—is providing me with something up front. Many do not, so I go through this process without any information about what I am doing. It is a real missed opportunity so far, but now we can right that to make sure that DVSs are providing at least basic information to the public about what to do, what not to do, what questions to ask and where to get help.

Q117 Chi Onwurah: Thank you very much for your evidence so far. It is going to be informative about the use of digital ID in recruitment. You said earlier that it helps to separate away from geography, which implied that the digital ID did not reference the location or the home address of the person who was being ID'd. What does the digital ID ID? Part of the reason behind that question is this: is it simply providing identification, or

[Chi Onwurah]

could it also be used as part of the triage process? Can that be done algorithmically, with some of the dangers that we see in algorithmic, automated decision making?

Keith Rosser: Those are several really good questions. I will use an example about location from the other perspective, first of all. At the moment, Home Office policy has not caught up with digital identity, and we are addressing that. There is a real opportunity to right that. It means that one in five work seekers right now cannot use digital identity to get a job, because they do not have an in-date British or Irish passport. If you have a visa or an in-date British or Irish passport, that is fine, but if you are among the one in five people in the country who do not have an in-date passport, you cannot. Those people have to visit the premises of the employer face to face to show their documents, or post their original documents across the UK.

This has really created a second-class work seeker. There are real dangers here, such as that an employer might decide to choose person one because they can hire them a week faster than person two. There is a real issue about this location problem. Digital identity could sever location to allow people more opportunities to work remotely across the UK.

There were really good questions about other information. The Bill has a provision for other data sharing. Again, there is the potential and the opportunity here to make UK hiring the fastest globally by linking other datasets such as HMRC payroll data. Rather than looking at a CV and wondering whether the person really worked in those places, the HMRC data could just confirm that they were employed by those companies.

There is a real opportunity to speed up the verification but, as I want to acknowledge and as you have referred to, there is certainly also a risk. Part of our mission is to make UK hiring fairer, not just faster and safer. I want to caution against going to a degree of artificial intelligence algorithmic-based hiring, where someone is not actually ever in front of a human, whether by Teams video or in person, and a robot is basically assessing their suitability for a job. We have those risks and would have them anyway without this Bill. It is really important as we go forward that we make sure we build in provisions somewhere to ensure that hiring remains a human-on-human activity in some respects, not a completely AI-based process.

The Chair: Mr Rosser, thank you very much indeed for your evidence this afternoon. We are grateful for your time, sir.

Examination of Witnesses

Helen Hitching and Aimee Reed gave evidence.

3.1 pm

The Chair: Welcome, ladies. We have until 3.30 pm for this session. Will the witnesses please be kind enough to introduce themselves to the Committee for the record? Let us start with Helen Hitching.

Helen Hitching: Good afternoon. I am Helen Hitching, Chief Data Officer for the National Crime Agency, and this is my first time in front of a Committee.

The Chair: Welcome and thank you. Aimee Reed?

Aimee Reed: Hello, everybody. This is also my first appearance in front of a Bill Committee. I am the Director of Data at the Metropolitan Police Service. For my sins, I also volunteer to lead all 43 forces on data; I am chair of the national police data board. I am here today in that capacity as well.

Q118 Stephanie Peacock: You are both very welcome. My first question is to Aimee. Currently, police are required by section 62 of the Data Protection Act 2018 to log their justification for accessing specific data records; this Bill, of course, changes that. How time consuming is that requirement currently for officers?

Aimee Reed: It is a big requirement across all 43 forces, largely because, as I am sure you are aware, we are operating on various aged systems. Many of the technology systems across the policing sector do not have the capacity to log section 62 requirements, so police officers are having to record extra justification in spreadsheets alongside the searches and release of information that they deliver. So the requirement is a considerable burden across all the forces.

Q119 Stephanie Peacock: Helen, how, if at all, will listing as a recognised legitimate interest

"detecting, investigating or preventing crime",

to quote the new definition, aid the tackling of serious crime in the UK?

Helen Hitching: Sorry—could you repeat that?

Stephanie Peacock: Sure. My understanding of the legislation in front of us is that if the Bill becomes law,

"detecting, investigating or preventing crime"

will be listed as a recognised legitimate interest and therefore be subject to separate, or slightly amended, data rules. How will that change help tackle serious crime in the UK?

Helen Hitching: I think it will bring a level of simplicity across the data protection environment and make sure that we can share data with our policing colleagues and other services in a more appropriate way. It will make the whole environment less complex.

Q120 Stephanie Peacock: I have a connected but slightly separate question. Would being able to apply for a joint designation notice with the intelligence services aid competent authorities in targeting serious and organised crime, and if so, how?

Helen Hitching: Yes, it will aid it. Again, it brings in the ability to put the data protection framework on the same level, so we can share data in an easier fashion and make it less complex.

Q121 Sir John Whittingdale: Can you say a little bit more about the implications of personal data sharing between countries, the extent to which that might lead to a lowering of standards of protection and how we safeguard against that?

Helen Hitching: The agency does not believe that those safeguards will be lowered. We will still not be able to share data internationally with countries that do not have the same standards that are met by the UK. It

will provide greater clarity about which regimes should be used and at which point. The standards will not reduce.

Q122 Sir John Whittingdale: You need to be satisfied that the third country maintains the same level of data protection standards that exists in the UK. To what extent has that been an impediment for data sharing?

Helen Hitching: The agency has had to undertake a test to make sure that there is adequate or, essentially, equivalent protection. That standard is now changing to "not materially lower", so it will be a lot easier to understand where those protection levels are the same as or not materially lower than the UK's. It will be simplified a lot.

Q123 Sir John Whittingdale: On a separate issue, at the moment we have a range of bodies responsible for different aspects of surveillance, such as the Biometrics Commissioner, the Investigatory Powers Commissioner and the Surveillance Camera Commissioner. Those are being brought together into either the Information Commissioner or the Investigatory Powers Commissioner. To what extent do you think that will improve the overall oversight of surveillance?

Aimee Reed: Policing thinks that that will significantly simplify things. It will not reduce the level of oversight and scrutiny that will be placed upon us, which is the right thing to do. In terms of the simplicity of that and the regimes that we are under, we are very supportive of that change.

Helen Hitching: Likewise, we are supportive and welcome the simplification. We do note, however, that the Biometrics Commissioner currently has a keen focus on developing technology in a legal manner and consults with the public. We would ask that there remains a focus on that oversight of biometrics, to assure the public that that work remains a priority once the regulation of biometrics transfers to the Information Commissioner's Office and to make sure that that focus is retained.

Q124 Damian Collins: How easy do you find it to gather data as part of investigations at the moment, particularly if you are working with companies that provide services to individuals? Do you think the provisions in the Bill will make that any easier?

Aimee Reed: On balance, it will make things easier. We are retaining the very different sections of the Act under which different organisations operate, and the sections that look to improve joint working across part 3 and part 4 agencies are very welcome. At the moment that is not about simplifying the relationships between those in, say, part 2 and part 3, albeit data sharing is entirely possible. In essence, it is going to get simpler and easier to share data, but without losing any of the safeguards.

Q125 Damian Collins: In terms of criminal investigations, practically how easy is it to get hold of data and information that you consider to be important, particularly if it is from private companies?

Aimee Reed: It is not as easy as we would like it to be, and provision is not made in the Bill to make that easier. There are some discussions about it going into the Online Safety Bill and other areas. It could be easier. We would push harder in the future, but at the moment, getting parity across the other areas and around national security is a focus that we welcome.

Helen Hitching: I want to pick up on the fact that safeguards are not reducing. It is key that the agency notes the point that our safeguards are not being lowered because of this.

Q126 Mark Eastwood (Dewsbury) (Con): I have been on the parliamentary police and fire service scheme, so I have spent a lot of time with the police. One of the big frustrations from the police's point of view is the lack of free flow of information, particularly when it concerns charging decisions, along with redaction, which potentially causes some antagonism between the two. I know this is not strictly covered in the Bill, but would it be beneficial to both parties if you were able to share unredacted information before a charging decision is made?

Aimee Reed: I will answer that in respect of where we are now in national policing. It would be of considerable benefit if the guidance was clearer that we could share information without having to redact it, certainly pre-charge, to enable better and easier charging decisions—to be honest—within the Crown Prosecution Service. It would also reduce the current burden on officers: you can think about the volume of data they have to hand over, and it can be video, audio, transcripts—it is not just witness statements, as it used to be 20 or 30 years ago. Reducing that burden would be significant for frontline officers and unleash them to be able to do other things.

Q127 Mark Eastwood: So it would be an advantage for the Government to look into including that.

Aimee Reed: It certainly would. It is not that we cannot do that now; I just think the guidance could be clearer. It would put it into sharper relief if we could release that burden from policing to the CPS and the CPS felt confident that that was within the rules.

Helen Hitching: The agency agrees with that—there would be the same impact.

Q128 Chi Onwurah: I think you implied that there was data that you would like to have access to but currently do not have access to. Can you elaborate on what data you do not have access to in terms of data sharing and the barriers? What would be helpful for investigations?

Aimee Reed: It is not so much about specific datasets; it is about synchronisation and the speed with which you can exchange data that enables you to make better decisions. Because the Data Protection Act is split into three parts, and law enforcement quite rightly has a section all of its own, you cannot utilise data analytics across each of the parts. Does that make sense? If we wanted to do something with Driver and Vehicle Licensing Agency data and automatic number plate recognition data, we could not join together those two large datasets to enable mass analysis because there would be privacy rights considerations. If want to search datasets from other parts of that Act, we have to do that in quite a convoluted administrative way that perhaps we can share within law enforcement. It is more about the speed of exchange.

Q129 Chi Onwurah: Is it about the speed of exchange with other Government agencies or with local government agencies?

Aimee Reed: It is more with our local partners. I am sure that our partners would say they are equally frustrated by the speed at which they can get data from the police in large datasets to enable them to make better decisions in their local authorities. That is just how that Act was constructed, and it will remain so. The recent ICO guidance on sharing has made that simpler, but this realm of the Bill will not make that synchronisation available to us.

Q130 Chi Onwurah: Do you think it should be available to you? Are there reasons why it is not available to you?

Aimee Reed: It is about getting right the balance between what we do with people's personal data and how the public would perceive the use of that data. If we just had a huge pot where we put everybody's data, there would be real concerns about that. I am not suggesting for a second that the police want a huge pot of everybody's data, but that is where you have to get the balance right between knowing what you have and sharing it for the right purpose and for the reason you collected it in the first place.

Q131 Chi Onwurah: Just to follow up on the questions about the different types of regulation, do you feel that the balance has been struck appropriately when it comes to biometric data, particularly for facial recognition, for example?

Helen Hitching: Sorry—could you repeat that?

Chi Onwurah: Has the balance between sharing and the regulation of biometric data, particularly facial recognition data, been struck in the right way?

Helen Hitching: I do not think facial recognition data is captured.

Aimee Reed: On facial recognition, given that we have deployed it—very high profile—I think that the balance is right. We have learned a lot from the South Wales judgment and from our own technical deployments. The Bill will also highlight how other biometric data should be managed, creating parity and an environment where biometric data that we do not yet have access to or use of is future-proofed in the legislation. That is really welcome.

Q132 Rebecca Long Bailey: Helen, you mentioned that you are broadly supportive of the abolition of the Biometrics Commissioner and the Surveillance Camera Commissioner, but that that abolition will not reduce the existing level of oversight. Now seems to be the time to request additional resources if you did not feel that the new commissioners would be adequately resourced, so do you have confidence that the Investigatory Powers Commissioner has sufficient resources and expertise to take on the functions it has to? Similarly, does the Information Commissioner have sufficient resources and expertise to oversee regulation in this area?

Helen Hitching: It is difficult for the agency to comment on another organisation's resources and capabilities. That question should probably be posed directly to them. The Information Commissioner's Office already deploys resources on issues related to law enforcement data processing, including the publication of guidance. From a biometrics perspective, the casework is moving to the IPC, so from a resourcing perspective I think it would have adequate casework provision and expertise.

Aimee Reed: I echo the comments about expertise, particularly of the Investigatory Powers Commissioner. I think that the expertise exists but, like Helen, whether it has enough resources to cope with the casework I presume is a demand assessment that it will do in response to the Bill.

Q133 Rebecca Long Bailey: I have a final question for you, Aimee. There are concerns, particularly given that the Information Commissioner's Office 2021 data protection audit report gave an assurance rating of "limited" to the Met's policies on records management. How can you reassure the public, given that there will be such an expansion of powers in the area, that the Met will not receive a similar report over the next 12 months?

Aimee Reed: That is a very topical question today. The first thing to say is that I am not sure I agree that this is a large expansion of our access to personal data; I think it is a simplification of the understanding of what we can do as a law enforcement body. All the same safeguards and all the same clear water will be in place between the different parts of the Act.

We did indeed get a "limited" rating on records management, but as I am sure you are aware, we were assessed on three areas, and we got the second highest grading in the other two: the governance and accountability of our management data; and our information risk management. They came out higher.

What have we done since 2021? We have done quite a lot to improve the physical and digital records management, with greater focus on understanding what data we hold and whether we should still hold it, starting a review, retain and deletion regime. We now have an information asset register and a ROPA—record of processing activities. The previous commissioner, Cressida Dick, invested a significant amount in data management and a data office, the first in UK policing. The new commissioner, as I am sure you have seen, is very committed to putting data at the heart of his mission, too. We have already done quite a lot.

The Bill will simplify how we are able to talk to the public about what we are doing with their data, while also reassuring them about how we use it. We are in a very different place from where we were 12 months ago; in another 12 months, it will be even more significantly improved. We have just worked with the Open Data Institute to improve how open we will be with our data to the public and partners in future, giving more to enable them to hold us to account. I am already confident that we would not get a rating like that again in records management, just based on the year's review we have had from the ICO about where we have got to.

Q134 Rebecca Long Bailey: Similarly, now that you have authority over all forces across the UK, I have the same question regarding each of them: are you content that they are equipped and resourced adequately to meet data protection requirements, given that there is such an expansion?

Aimee Reed: I wish I had authority across them. I represent—that is a better way of describing what I do. Am I confident that law enforcement in general has the right investment in this space, across all forces? No, I am not. That is what I am working hard to build with Chief Constable Jo Farrell, who leads in this area for all

forces on the DDaT approach. Am I more confident that forces really getting investment in this space is necessary? Absolutely.

Q135 Rebecca Long Bailey: In terms of additional resources, are there any specific figures or requirements that you could point the Government towards at this stage?

Aimee Reed: In line with our own DDaT framework, we are working with the Home Office and other ministerial bodies on what good looks like and how much is enough. I am not sure that anybody has the answer to that question yet, but we are certainly working on it with the Home Office.

The Chair: Ladies, thank you very much indeed for your time this afternoon. We will let you get back to your crime fighting.

Examination of Witnesses

Andrew Pakes and Mary Towers gave evidence.

3.21 pm

The Chair: We now come to our ninth panel. We welcome Andrew Pakes, who is director of communications and research at Prospect, and Mary Towers, who is the policy officer at the Trades Union Congress. We have until 3.55 for this session. I invite the witnesses to introduce themselves to the Committee for the record—ladies first.

Mary Towers: Hi, and thanks very much for inviting the TUC to give evidence today. My name is Mary Towers. I am an employment rights policy officer at the TUC, and I have been leading a project at the TUC looking at the use of AI in the employment relationship for the past couple of years.

Andrew Pakes: Hello, everyone. Thank you for inviting Prospect to give evidence today. My name is Andrew Pakes. I am one of the deputy general secretaries and the research lead for Prospect union, which represents scientific, technical and professional workers. I am also a member of the OECD's AI expert panel, representing trade unions.

Q136 Stephanie Peacock: Good afternoon to you both; you are very welcome. My first question is to Andrew. Obviously, the nature of work has changed significantly over the past few decades, particularly in the last decade. What impact has technology, particularly the rise of automated decision making and automated performance management, had on the workplace?

Andrew Pakes: We were already seeing a huge change in the use of digital technology prior to the pandemic. The pandemic itself, not least through all the means that have kept many of us working from home, has transformed that. Our approach as a trade union is to embrace technology. We believe that our economy and the jobs our members do can be made better and more productive through the good deployment of technology to improve jobs.

We also think there is a downside to it all. Everything that needs to be risked and balanced is in that. Alongside the advance in innovation and technology that has brought benefits to the UK, we have seen a rise in the darker or less savoury side of that, which is namely the rise of surveillance software; the ability of software to follow us, including while working from home, and to micromanage us and track people; and the use of technology in performance management—the so-called people analytics or HR management, which is largely an unregulated area.

If you ask me which legislation this should sit in, I would probably say an employment-type Bill, but this is the legislation we have and the Government's choice. We would definitely like to see checks and balances at least retained in the new legislation compared with GDPR, but maybe they should be enhanced to ensure that there is some form of social partnership and that working people have a say over how technology is introduced and implemented in their workspaces.

Q137 Stephanie Peacock: That makes sense. You mentioned the changes since the pandemic. How do you think those changes have impacted on the right to privacy and the right to a work-life balance? I presume that has shifted since the pandemic.

Andrew Pakes: There is increasing evidence that while technology has allowed many of us to remain connected to our workspaces—many of us can now take our work anywhere—the downside is that our work can follow us everywhere. It is about the balance of digital disconnection and the ability to switch off from work. I am probably preaching to the wrong crowd, because MPs are constantly on their phones and other technology, but many of us are able to put that away, or should do, because we are contracted workers and have a different relationship with our workplace in terms of how that balance is struck. We very much focus on wellbeing and on information and consultation, ensuring that people are aware of the information that is collected on us.

One of the troubling factors that we and the TUC have picked up is that consistently, in opinion polls and research that is done, working people do not have confidence or knowledge about what level of data is being collected and used on them. When we see the increasing power of technology through AI and automated decisions, anxiety in the workplace is best foiled by transparency, in the first place, and, we would obviously argue, a level of social partnership and negotiation over how technology is introduced.

Q138 Stephanie Peacock: What effect do you believe the new rules in the Bill on automated decision making will have on workers? I think you have alluded to this, but would you like to see greater protections in place?

Andrew Pakes: Absolutely. What strikes me about the legislation you are considering is that just about all our major competitors—who are more productive and more advanced, often in innovation, including the United States—are choosing a path of greater scrutiny and accountability for AI and automated decision making. There is a concern that in this legislation we are taking an alternative path that makes us stand out in the international economy, which is about diluting existing protections we have within GDPR to a lower level. That raises concerns.

We have particular concerns about automated technology, but also about the clauses on the reduction of powers around data protection impact assessments. We think

the risk is that the legislation could open the back door to the increase in dodgy surveillance and other forms of software coming into the UK market. I am worried about that for two reasons: first, because of the impact it has on individual workers and what is happening there; and secondly, because most of this technology—we have been part of a project that has tracked over 500 different surveillance software products currently on the international market—is designed largely for a US or Chinese market, with little knowledge of how it is being done.

What we know through ensuring consultation on the existing DPIA arrangements is that there is a break in the current rules that enables or ensures that employers have a consultation and check where their products are taking their data from and what they have stored. Diluting that risks ensuring that we are not sure where that data is being used and we are not sure of the power of this technology, and working people then end up with a worse deal than they currently have.

Q139 Stephanie Peacock: I have a couple of questions for Mary Towers. Do you think that the changes in the Bill will do anything to improve the collective rights of workers? If not, what sort of mechanisms would you like to see in place to give workers a method of redress collectively?

Mary Towers: On the contrary, we would say that the Bill in fact reduces the collective rights of workers, particularly in relation to data protection impact assessments. As Andrew has mentioned, at the moment the right to a data protection impact assessment involves an obligation on an employer to consult with workers or their representatives. That is an absolutely key tool for trade unions to ensure that worker voice is represented in the path of the introduction of new technologies at work. Also, at the moment, missing from the Bill is the ability of trade unions to act as representatives for data subjects in a collective way. We say that that, too, is missing, could be added and would be an important role that unions could take on.

Another aspect missing from the Bill, which we say is a hugely missed opportunity, is a potential right that workers could have to have an equal right to their data that matches the right employers have over worker data. Once workers had that right, they could then collectivise their own data, which would enable them, for example, to pick up on any discriminatory patterns at work or pick up any problems with equal pay or the gender pay gap. We say that that right to collectivise data and redress the imbalance of power over data at work is really important.

The Bill misses entirely the opportunity to introduce those kinds of concepts, which are actually vital in the modern workplace, where data is everything. Data is about control; data is about influence; data is the route that workers have to establish fair conditions at work. Without that influence and control, there is a risk that only one set of interests is represented through the use of technology at work, and that technology at work, rather than being used to improve the world of work, is used to intensify work to an unsustainable level.

Q140 Stephanie Peacock: In that answer, you highlighted the imbalance between employers and workers. Correct me if I am wrong, but you said that data protection impact assessments are particularly valuable to both trade unions and the collective workforce. Do you have any specific examples of this consultation tool being used successfully?

Mary Towers: Yes. This is something that Andrew's union, Prospect, has been really active in. It has produced some absolutely brilliant guidance that looks in detail at the importance of the process of data protection impact assessments and rolled out training for its trade union reps. Again, several of our other affiliates have undertaken that really important work, which is then being rolled out into the workplace to enable reps to make good use of that process.

I will, however, add the caveat that I understand from our affiliates that there is a very low level of awareness among employers about that obligation, about the importance of that process and about exactly what it involves. So a really important piece of awareness-raising work needs to be done there. We say it is vital to build on the existing rights in the UK GDPR, not dilute or remove them.

Q141 Stephanie Peacock: What impact would the Bill have on workers by taking away this tool or watering down the DPIAs into assessments of high risk, especially given that earlier today, before this Committee, the Information Commissioner himself raised concerns about the lack of clarity on what will count as high-risk processing? That question is to either of you, briefly. I have one more and then I will let someone else come in.

Andrew Pakes: We would assert that under the law of GDPR, high risk in the legislation is, I think, in recital 39. I will correct that if I picked the wrong one. It talks about high risk as being decisions that can make material or non-material impact on people. If we now have software and algorithms or automated decisions that can hire and fire us—we have examples of that—and can decide who deserves a promotion or who can be disciplined, if that information can now be used to track individuals and decide whether someone is a good or bad worker, we would assert that that is a high risk. Anything that can actually affect both your standing in your workspace or your contractual relationship, which is essentially what employment is, or which has an impact on the trust and confidence the employer has in you and, equally, your trust and confidence back in the employer, that is a very clear definition of high risk.

What is important about the existing UK GDPR is that it recognises the nature of high risk but, secondarily, it recognises that data subjects themselves must be consulted and involved either directly or, where that is not practicable, through their representatives. Our worry is that the legislation that is tabled now dilutes that and opens up risk to bad practice.

Q142 Stephanie Peacock: Thank you. This is my final question. Does the Bill offer enough detail on the new threshold for charging or refusing a subject access request that is either "vexatious or excessive" to assure workers that they will still be able to access their personal records from an employer when making a good-faith request?

Mary Towers: The right to a data subject access request—again, like the DPIAs—is an absolutely crucial tool for trade unions in terms of establishing transparency over how their data is being used. Really, it provides a

route for workers and unions to get information about what is going on in the workplace, how technologies operate and how they are operating in relation to individuals. It is an vital tool for trade unions.

What we are concerned about is that the new test specified in the Bill will provide employers with very broad discretion to decide when they do not have to comply with a data subject access request. The use of the term "vexatious or excessive" is a potential barrier to providing the right to an access request and provides employers with a lot of scope to say, for example, "Well, look, you have made a request several times. Now, we are going to say no." However, there may be perfectly valid reasons why a worker might make several data subject access requests in a row. One set of information that is revealed may then lead a worker to conclude that they need to make a different type of access request.

We say that it is really vital to preserve and protect the right for workers to access information. Transparency as a principle is something that, again, goes to really important issues. For example, if there is discriminatory operation of a technology at work, how does a worker get information about that technology and about how the algorithm is operating? Data subject access requests are a key way of doing that.

Q143 Sir John Whittingdale: May I ask a relatively simple question? Obviously your concern is the protection of workers' rights, and safeguards against discrimination and other potential adverse consequences of technology. We will debate the provisions of the Bill in those areas in the coming weeks—I suspect at some length—but would you nevertheless accept that the overall impact of the legislation, if we get this right, will be beneficial to your members in terms of the promotion of growth and potential future job opportunities?

Andrew Pakes: "If we get this right" is doing a lot of heavy lifting there; I will leave it to Members to decide the balance. That should be the goal. There is a wonderful phrase from the Swedish trade union movement that I have cited before: "Workers should not be scared of the new machines; they should be scared of the old ones." There are no jobs, there is no prosperity and there is no future for the kind of society that our members want Britain to be that does not involve innovation and the use of new technology.

The speed at which technology is now changing and the power of this technology compared with previous periods of economic change make us believe that there has to be a good, robust discussion about the balances of checks and balances in the process. We have seen in larger society—whether through A-level results, the Post Office or other things—that the detriment is significant on the individuals impacted if legislators get that balance wrong. I agree with the big principle and I will leave you to debate that, but we would certainly urge that checks and balances need to be balanced, not one-sided.

Mary Towers: Why does respect for fundamental rights have to be in direct conflict with growth and innovation? There is not necessarily any conflict there. Indeed, in a workplace where people are respected, have dignity at work and are working in a healthy way, that can only be beneficial for productivity and growth.

Q144 Damian Collins: I have been listening carefully to what you have been saying and it strikes me that there are two issues: the use of technology in the general workplace, and the rights of workers who work through technology to do their jobs. In the workplace itself, data gathering and analysis has always existed to some extent. If we were having this conversation in the 1960s, we would have been talking about people doing time-motion studies of people in factories to work out what efficiency looked like. Is your concern in respect of a general working environment that employers are transparent about what sort of data they gather and how they use it?

Andrew Pakes: That is the first base. The power of technology is changing so quickly, and the informal conversations we have every day with employers suggest that many of them are wrestling with the same questions that we are. If we get this legislation right, it is a win-win when it comes to the question of how we introduce technology in workspaces.

You are right to identify the changing nature of work. We would also identify people analytics, or the use of digital technology to manage people. How we get that right is about the balance: how do you do it without micromanaging, without invading privacy, without using technology to make decisions without—this is a horrible phrase, but it is essentially about accountability—humans in the loop? Good legislation in this area should promote innovation, but it should also have due regard to balancing how you manage risks and reduce harms. That is the element that we want to make sure comes through in the legislation in its final form.

Q145 Damian Collins: So you do not have an in-principle objection to the use of technology to monitor the efficiency, output and performance of employees within a working environment, but you think it needs to be based on agreed criteria—that employers need to be transparent about how they are gathering data and what they are using it for.

Andrew Pakes: Absolutely. Let me give you a quick example of one piece of technology that we have negotiated in some areas: GPS tracking. It might be old technology, compared with many things that you are looking at. We represent frontline workers who often work alone, outside, or in spaces where their work could be risky. If those people cannot answer their radio or phone, it is in the legitimate interests of all of us to see where they are, in case they have had an accident or are in a dangerous situation. We can see a purpose to that technology. In negotiation with employers, we have often said, "This is good technology for keeping people safe, but we are not happy with it being used in performance reviews." We are not happy with people saying, "I am sorry, Mr Collins, but you seem to spend a lot of time in the same café each lunch time."

The issue is not the technology, but its application. Technology that is used to increase safety is very good, but the risk is that it will be used to performance-manage people; employers may say, "You are not doing enough visits," "You aren't working fast enough," or, "You don't drive fast enough between jobs." We need balance and control, as opposed to ruling out technology that can keep people safe and well.

Q146 Damian Collins: For some people, their job is done through technology. Take a gig economy worker working for a delivery company. Do you have concerns about how app developers design their systems and

[Damian Collins]

their relationship to the worker? For example, you may work for a company that does not pay you for your waiting time. You are not working contracted hours; you are working in the gig economy, on a "turn up and get paid" basis. The system may have been designed to favour people who are always on the app and always ready for work, even if they are not being paid for that, over people who log on only at particular times. The app developer may not be very transparent about that, because they do not want to be named and shamed for treating their workers that way. Good and bad employers would say that there are people working to different standards, but do you feel that there is still a lack of transparency in the gig economy about how different apps process and use data, and the impact that has on the day-to-day working life of the people who use those apps?

Andrew Pakes: From my perspective, yes.

Mary Towers: The TUC has red lines relating to the use of these types of technologies. One is that we simply should not have technologies at work that are not transparent and that operate in a way that people do not understand. The principle of explainability is really important to us. People need to understand when the technologies are operating, and how they operate in relation to them. On top of that, it is absolutely vital that discriminatory data processing does not take place. The example that you gave from the gig economy is potentially of a discriminatory pay calculation—of an algorithm that might be calculating different rates of pay for individuals who are carrying out exactly the same work. The algorithm is potentially replicating existing inequalities in pay that are rooted in gender or race.

Q147 Damian Collins: The issue is not different rates of pay per task, but the amount of paid work that someone might get within a period.

Mary Towers: Yes. Drivers are a good example. People drive a certain distance to pick people up or deliver items. Even when the driving time is exactly the same, people may be paid different rates, because the algorithm will have worked out how long certain groups of people are likely to wait before they accept a gig, for example. I emphasise that, in our view, those sorts of issues are not restricted to the gig economy; they spread way beyond it, into what one might consider to be the far more traditional professions. That is where our red lines are. They relate to transparency, explainability, non-discrimination and, critically, worker and union involvement at each stage of the AI value chain, including in the development of that type of app—you mentioned development. Unless the worker voice is heard at development stage, the likelihood is that worker concerns, needs and interests will not be met by the technology. It is a vital principle to us that there be involvement of workers and unions at each stage of the AI value chain—in development, application and use.

Q148 Chi Onwurah: Welcome to both of you. Apologies for my misuse of my own technology earlier.

The Minister talked about the need for growth, which has been sadly lacking in our economy for the last 13 years. Obviously, technology can make huge improvements to productivity for those in the workforce. Mr Pakes, as someone whose members are involved in technology, scientific and IT organisations, I wonder whether you would agree with this, which comes from my experience in the diffusion of technology. Is it possible to get the best from technology in an organisation or company without the people who will be using it, or the people on whom it will be used, being an active part of that diffusion of technology, and understanding and participating in its use?

Andrew Pakes: Absolutely. That has always been how productivity has improved or changed, in effect, the shop floor. If you are asking, "What problems are you using technology to solve?", it may well be a question better asked by the people delivering the product or service than necessarily the vendor selling the software, whether that is old or new technology. I encourage the Committee to look at the strong evidence among our competitors who rate higher, in terms of productivity and innovation, than the UK, where higher levels of automation in the economy are matched by higher levels of worker participation. Unions are the most common form, but often it can be works councils or small businesses in terms of co-design and collaboration. We see that social partnership model of the doers, who identify and solve problems, being the people who do that.

We have good examples. We represent members in the nuclear sector who are involved in fusion, small modular reactors or other technology, where the employer-union relationship is critical to the UK's intellectual property and the drive to make those successful industries. In the motor industry and other places where the UK has been successful, we can see that that sense of social partnership has been there. We have examples around using AI or the monitoring of conversations or voices. Again, I mentioned GPS tracking, but in safety-critical environments, where our members want to be kept safe, they know that technology can help them. Having that conversation between the workforce and the employer can come up with a solution that is not only good for our members, because they stay safe and understand what the safety regime is, but good for the employer, because days are not lost through illness or accidents. For me, that sense of using legislation like this to underpin good work conversations in the data setting is what the mission of this Bill should be about.

Q149 Chi Onwurah: In terms of data sharing, should there be provisions in the Bill to ensure that workers can give free and informed consent to the sharing of their data, or will the asymmetry of the relationship in the employment contract make that challenging?

Andrew Pakes: We think there should be a higher bar, because of the contractual nature. Whether it is self-employed workers contracting for a piece of work or an employment relationship, there is a fundamental difference in our view between my individual choice to go online and enter my data into a shop, because I want to be kept appraised of when the latest product is coming out—it is my free choice to do that—and my being able to consent in an employment relationship about how my data is used. As Mary said, the foundation stone has to be transparency on information in the first place. Beyond that, there should be negotiation to understand how that data is used.

The critical point for us is that most companies in the UK are not of a size where they will be developing their own AI products—very few will be; we can probably name a couple of them. Most companies using automated decisions or AI will be purchasing that from a global marketplace. We hope many of them will be within certain settings, but we know that the leaders in this tend to be the Chinese market and the US market, where they have different standards and a range of other things. Ensuring that we have UK legislation that protects that level of consent and that redresses that power balance between workers and employers is a critical foundation to ensuring that we get this right at an enterprise level.

Q150 Chi Onwurah: Have you identified any provisions to achieve that in the Bill as it stands?

Andrew Pakes: We would like to see more. We are worried that the current legislation, because of things such as DPIAs, drops that level of standards, which means that the UK could end up trading on a lower standard than other countries, and that worries us.

Mary Towers: We are also concerned about the change to the test for international data transfers, which might make the requirements less restrictive. There is a change from adequacy to a more risk-based assessment process in terms of international data transfers. Again, we have very similar concerns to Andrew about the use of technologies rooted in international companies and the inevitable international transfers of data, and workers essentially losing control over and knowledge of what is happening with their data beyond the workplace.

In addition, I would also like to make a point about the importance of transparency of source code, and the importance of ensuring that international trade deals do not restrict that transparency, meaning that workers cannot access information about source code once data and AI-powered tools are rooted in other countries.

Q151 Mark Eastwood: I would like to declare, again, that I am a member of Prospect, and therefore I have a bit of skin in the game on this one. You mentioned GPS and surveillance technology. Very quickly, could you give me an idea of the current scale of that? Are the majority of employers going down this route? If this Bill is pushed through, could you give me an idea of how usage could increase or decrease, depending on how you see the outcome of the Bill?

Mary Towers: I will give my statistics very quickly. Our polling revealed that approximately 60% of workers perceived that some form of monitoring was taking place in their workplace. The CEO of IBM told Bloomberg last week that 30% of non-customer facing roles, including HR functions, could be replaced by AI and automation in the next five years.

A recent report from the European Commission's Joint Research Centre—the "Science for Policy" report on the platformatisation of work—found that 20% of German people and 35% of Spanish people are subject to algorithmic management systems at the moment. Although that is obviously not UK-based, it gives you a very recent insight on the extent of algorithmic management across Europe.

Andrew Pakes: And that matches our data. Around a third of our members say that they are subject to some form of digital monitoring or tracking. That has grown, particularly with the rise of hybrid and flexible working, which we are in favour of. This is a problem we wish to solve, rather than something to stop, in terms of getting it right.

Over the past two years, we have increasingly seen people being performance managed or disciplined based on data collected from them, whether that is from checking in and out of buildings, their use of emails, or not being in the right place based on tracking software. None of the balances we want should restrict the legitimate right of managers to manage, but there needs to be a balance within that. We know that using this software incorrectly can micromanage people in a way that is bad for their wellbeing.

The big international example, which I will give very quickly, is that if you look at a product like Microsoft—a global product—employers will buy it. My work computer has Office 365 on it. Employers get it on day one. The trouble with these big products is that, over time, they add new products and services. There was an example where Microsoft did bring in a productivity score, which could tell managers how productive and busy their teams were. They rowed back on that, but we know that with these big, global software projects—this is the point of DPIAs—it is not just a matter of consultation on day one.

The importance of DPIAs is that they stipulate that there must be regular reviews, because we know that the power of this technology transforms quickly. The danger is that we make life miserable for people who are good, productive workers and cause more problems for employers. It would be better for all of us to solve it through good legislation than to arm up the lawyers and solve it through the courts.

The Chair: I am afraid that we are subject to chronological monitoring, so we must bring this session to an end. I thank our two representatives very much indeed for their evidence this afternoon; we are grateful for your time. We will now move on to our 10th panel.

Examination of Witnesses

Alexandra Sinclair, Ms Laura Irvine and Jacob Smith gave evidence.

3.55 pm

The Chair: Welcome to the witnesses in our 10th panel. Thank you for your time this afternoon. We will hear from Alexandra Sinclair, a research fellow at the Public Law Project; Laura Irvine, via Zoom, the convener of the privacy law sub-committee at the Law Society of Scotland; and Jacob Smith, the UK accountability team leader at Rights and Security International. We have until 4.25 pm for this session. Would the witnesses please be kind enough to introduce themselves to the Committee for the record, starting with those in the room?

Alexandra Sinclair: Thank you to the Committee for inviting me. My name is Alexandra Sinclair and I am a research fellow at the Public Law Project. The Public Law Project is an access to justice charity. We help people to seek redress for unfair or unlawful decisions made by public authorities. I am also a doctoral researcher at the London School of Economics where my research focuses on automated decision making.

Jacob Smith: My name is Jacob Smith. I am the UK accountability team leader at Rights and Security International, a London-based charity aimed at the intersection between national security and human rights, which tries to ensure that when Governments take pledges in the name of national security, they comply with human rights. I am also an associate lecturer in international law, privacy and data governance at the University of Surrey.

Ms Irvine: I am Laura Irvine. I am the convener of the privacy law sub-committee at the Law Society of Scotland. My day job is head of regulatory law at Davidson Chalmers Stewart—a Scotland-based law firm. I have been working in the field of data protection law for the past 10 years, so pre-GDPR and obviously, more recently, in a post-GDPR world.

The Chair: Thank you. You are all very welcome.

Q152 Stephanie Peacock: My first question is to Alexandra. What would the benefit be to the general public of the Government being transparent about their use of algorithms?

Alexandra Sinclair: Thank you for the question. In order for the public to have trust and buy-in to these systems overall, so that they can benefit from them, they have to believe that their data is being used fairly and lawfully. That requires knowing which criteria are being used when making a decision, whether those criteria are relevant, and whether they are discriminatory or not. The first step to accountability is always transparency. You can know a decision is fair or lawful only if you know how the decision was made in the first place.

Q153 Stephanie Peacock: That is great. Could you tell us about your TAG transparency register and what it revealed about the level of transparency in Government algorithmic use?

Alexandra Sinclair: Currently the Government have their algorithmic reporting transparency standard—I think I have got that right; they keep changing the acronym. Currently on that system there are about six reports of the use of automated decision-making technology in government. The Public Law Project decided to create a parallel register of the evidence that we could find for automated decision making in government. Our register includes over 40 systems in use right now that involve partly automated decisions about people. It would be great if the Government themselves were providing that information.

Q154 Stephanie Peacock: In the consultation, the Government said:

"There are clear benefits to organisations, individuals and society in explaining algorithmic decision-making"

in the public sector. Do you think that measures in the Bill achieve that? Do they unlock benefits and explain the Government's algorithmic decision making to the public?

Alexandra Sinclair: No, and I think they do not do that for three reasons, if I have the time to get into this. The changes to subject access requests, to data protection impact assessments and to the prohibition on article 22 are the key issues that we see. The reason why we are particularly worried about subject access requests and data protection impact assessments is that they are the transparency provisions. They are how you find out information about what is happening. A subject access request is how you realise any other right in the Bill. You can only figure out if an error has been made about your data, or object to your data, if you know how your data is being used in the first place.

What we are worried about with the Bill is that you currently have an almost presumptive right to your data under a subject access request, but the change in the Bill changes the standard from the current "manifestly unfounded or excessive" to "vexatious or excessive". It also gives a whole load of factors that data controllers are now allowed to take into account when declining your request for your own data. Furthermore, under the proposal in the Bill they do not have to give you the reason why they declined your request for the data. We think that is really problematic for individuals. You have got this information asymmetry there, and it is going to be really difficult for you to prove that your request was not vexatious or excessive if you do not even know why it was denied in the first place.

If we think about some examples that we have been talking about in Committee today, in a lot of the Uber and Ola-led litigation, where individuals were able to show that their employment rights had been unfairly treated, they were able to find out about that through subject access requests. Another example is the London Met police's gangs matrix. The Information Commissioner's Office did a review of that matrix and found that the system did not even clearly distinguish between victims and perpetrators of crime, and the only way for individuals to access the matrix and check if the information held on them is accurate is through a subject access request. That is our first concern with the Bill.

Our second concern is the changes to data protection impact assessments. The first thing to note is that they already have to apply only in high-risk processing situations, so we do not think that they are an undue or onerous burden on data controllers because they are already confined in their scope. What a data protection impact assessment does—this is what we think is beneficial about it—is not to be a brake on processing, but to force data controllers to think though the consequences of processing operations. It asks data controllers to think, "Where is that data coming from? What is the data source? Where is that data being trained? For what purpose is that data being used?" The new proposal under the Bill for data protection impact assessments significantly waters down those obligations and means that, essentially, the only requirement is accounting for the purposes for the data. So instead of explaining how the data is being used, you are only requiring that purpose.

We think that has two problems. First, data controllers will not be thinking through all the harms and consequences before they deploy a system. Secondly, if individuals affected by those systems want to get information about how their data was processed and what happened, there will be a lot less information on that impact assessment for them to assess the lawfulness of that processing.

My final critique of the Bill is this. We would say that the UK is world-leading in terms of article 22—other states are certainly looking to the UK—and it is a

strange time to be looking to roll back protections. I do not know if Committee members have heard about how Australia recently experienced the Robodebt scandal, on which there is a royal commission at the moment. In that case, the system was a solely automated debt discrepancy system that ended up making over 500,000 incorrect decisions, telling people that they had committed benefit fraud when they had not. Australia is having to pay millions of dollars in compensation to those individuals and to deal with the human cost of that decision. The conversation in Australia right now is, "Maybe we should have article 22. Maybe this wouldn't have happened if we had had a prohibition on solely automated decision making." When other states are looking to beef up their AI protections, we need to think carefully about looking to roll them back.

Q155 Stephanie Peacock: Thank you for that really comprehensive answer.

Jacob, what measures do you think should be in place to ensure that data protection legislation balances the need to protect national security with the need to uphold human rights? Does the Bill strike the right balance?

Jacob Smith: Thanks for the question. To take the second part first, we argue that the Bill does not strike the right balance between protecting national security and upholding data and privacy rights. We have three main concerns with how the Bill sets out that balance at the moment, and they come from clauses 24 to 26.

We have this altered regime of national security certificates for when law enforcement is taking measures in the name of national security, and we have this new regime of derogation notices. When law enforcement and the security services are collaborating, the notices allow the law enforcement body working in that collaboration to benefit from the more relaxed rules that are generally only for the intelligence services.

From our perspective, there are three main concerns. First, we are not quite sure why these amendments are necessary. Under human rights law, for an interference with somebody's data or privacy rights to be lawful, it needs to be necessary, and that is quite a high standard. It is not something akin to it being more convenient for us to have access to this data, or more efficient for us to have access to this data; it has to meet a high standard of strict necessity. Looking through the Second Reading debate, the impact assessment and the European convention on human rights analysis, there is no reference to anything that would be akin to necessity. It is all, "It would be easier for law enforcement to have these extra powers. It would be easier if law enforcement were potentially able to use people's personal data in more ways than they are at the moment." But that is not the necessity standard.

The second concern is the lack of safeguards in the Bill. Another thing that human rights law—particularly article 8 of the ECHR—focuses on is the necessity of introducing additional safeguards to prevent the misuse of legislation that allows public bodies to interfere with people's privacy rights. At the moment, as the Bill sets out, we have very weak safeguards when both national security certificates and designation notices are in place. At the moment, there is an opportunity, at least on the face of the Bill, for both those measures to be challenged before the courts. However, the issue here is that the Secretary of State has almost a monopoly over deciding whether those notices and certificates get published. So yes, although on the face of the Bill an individual may be able to challenge a national security certificate or a designation notice that has impacted them in some way, in practice they will not be able to do that if they do not know that it exists.

Finally, one encompassing issue is the expansive powers for the Secretary of State. One thing that we advocate is increased independent oversight. In the Bill, the Secretary of State has an extremely broad role in authorising law enforcement bodies to process personal data in a way that would otherwise be unlawful and go further than the existing regimes under the Data Protection Act 2018. Those are our three broad concerns in that regard. Ultimately, we do not see that the right balance has been made.

Q156 Stephanie Peacock: My final question is to all the witnesses. What are your views on the reforms to the ICO and their potential impact on its independence from Government?

Ms Irvine: We have concerns about the proposed changes and their potential impact on the independence of the Information Commissioner. I was able to listen to John Edwards speaking this morning, and I noted that he did not share those concerns, which I find surprising. The ICO is tasked with producing statutory codes of conduct, which are incredibly useful for my clients and for anyone working in this sector. The fact that the Secretary of State can, in effect, overrule these is concerning, and it must be seen as a limit on the Information Commissioner's independence.

That leads to a concern that we have in relation to the adequacy decision that is in place between the EU and the United Kingdom. Article 52 of the GDPR states very clearly that a supervisory authority must have clear independence. The provisions relating to the independence of the Commission—the potential interference of the Secretary of State in law is enough to undermine independence—are therefore of concern to us.

Alexandra Sinclair: We would just say that it is not typical for an independent regulator to have its strategic objectives set by a Minister, and for a Minister to set those priorities without necessarily consulting. We consider that the ICO, as subject matter experts, are probably best placed to do that.

Jacob Smith: From our perspective, the only thing to add is that one way to improve the clauses on national security certificates and designation notices would be to give the ICO an increased role in oversight and monitoring, for instance. Obviously, if there are concerns about its independence, we would want to consider other mechanisms.

Q157 Carol Monaghan (Glasgow North West) (SNP): Laura Irvine, in your briefing about the Bill you raised concerns about some of the language. We had some discussion this morning about the language and particular terms, such as what "vexatious" means, for example. Could you elaborate on your concerns?

Ms Irvine: Certainly. There are terms that have been used in data protection law since the 1984 Act. They were used again in the 1998 Act, echoed under the GDPR and included in all the guidance that has come from the Information Commissioner's Office over the past number of years. In addition to that, there is case law that has interpreted many of those terms. Some of

the proposed changes in the Bill introduce unexpected and unusual terms that will require interpretation. Even then, once we have guidance from the Information Commissioner, that guidance is sometimes not as helpful as interpretation by tribunals and courts, which is pretty sparse in this sector. The number of cases coming through the courts is limited—albeit that there is a lot more activity in the sector than there used to be. It simply presents a lot more questions and uncertainty in certain ways.

For my business clients, that is a great difficulty, and I certainly spend a lot of time advising clients on how I believe a matter—a phrase—will be interpreted, because I have knowledge of how data protection law works in general. That is based on my experience of the power of businesses and organisations, particularly in the third sector. Smaller bodies will often be challenged by a lack of knowledge and expertise, and that is a difficulty of introducing in legislation brand-new terms that are not familiar to practitioners, far less the organisations asked to implement the changes.

Q158 Carol Monaghan: You also raised concerns about automated decision making. Again, we have heard quite a lot about that today. You talked about a case on automated decision making, with regard to benefit awards being made by local authorities. Can you tell us a bit about that and where the danger might lie here?

Ms Irvine: I expect that you have heard a lot of warnings about safety. I echo what Alexandra said earlier about the removal of the right not to have automated decisions taken by organisations. That is something that we were concerned to see in a society where this is happening more and more. The particular example that we gave came from a study that had been carried out by the Equality and Human Rights Commission. That was looking particularly at decision making in local authorities; at how AI or algorithms were being used to take decisions without enough transparency; and at whether this gave the individuals the right to challenge those decisions, which stems from the transparency that is built in. The challenge for any organisation using any automated decision making—particularly in the public sector, I would submit, where the impact can be extremely significant, particularly if we are talking about benefits—is making sure these organisations understand what the technology is doing, explaining that to individuals and giving them the right to object.

The changes in the Bill relax the restrictions on automated decision making and allow that to happen almost as a default, with safeguards as an add-on, whereas article 22 as currently drafted provides a right not to have automated decisions taken about an individual unless certain circumstances apply. To echo what Alexandra said, when more and more decisions are being made automatically without a human intervening, and certainly without a human intervening at the appropriate stage to prevent damage or harm to individuals, it would absolutely seem like the wrong time to make these changes and relaxations to the regime.

Carol Monaghan: Thank you.

The Chair: You have all been superstars in our 10th panel. Thank you very much indeed for the evidence you have given this afternoon. We will now move on to the next panel.

Examination of Witness

Alex Lawrence-Archer gave evidence.

4.17 pm

The Chair: We now come to our 11th and final panel. We are pleased to welcome Alex Lawrence-Archer, who is a solicitor for AWO. We have until 4.40 pm for this session. Alex, will you please introduce yourself to the Committee for the record?

Alex Lawrence-Archer: Hi, I am Alex Lawrence-Archer. I am a solicitor and I litigate data rights cases at AWO. We were also instructed by Reset to help it to formulate its written evidence to the Committee, which hopefully you have received in the last couple of days.

The Chair: Thank you and welcome.

Q159 Stephanie Peacock: What are the main implications of the Bill for people's personal data rights?

Alex Lawrence-Archer: There is a group of changes in the Bill that, perhaps in ways that were unintended or at least not fully thought through, quite seriously undermine the protection of individuals' privacy and data rights. A few of the most concerning ones are the change to the definition of personal data, recognising legitimate interests, purpose limitation, changes to the test for the exercise of data subject rights—I could go on. You will have heard about many of those today. It amounts to an undermining of data rights that seems not to be in proportion to the relatively modest gains in terms of reduction in bureaucracy on the part of data controllers.

Q160 Stephanie Peacock: Following on from that answer, what do you think the impact will be of the new definition of personal data as contained in the Bill?

Alex Lawrence-Archer: It is quite difficult to predict, because it is complicated, but it is foundational to the regime of data protection. One of the issues is that in seeking to relieve data controllers of certain bureaucratic requirements, we are tinkering with these really foundational concepts such as lawful basis and the definition of personal data.

Two things could happen, I think. Some quite bad-faith arguments could be run to take quite a lot of processing outside the scope of the data protection regime. Although I doubt that those arguments would succeed, there is an additional issue; it is quite complicated to explain, but I will try. If it is unlikely but possible that an individual might be re-identified from a pseudonymised dataset—it could happen if there were a hack, say, but it is unlikely—that processing under the new regime would not, as the Bill is drafted, benefit from the protection of the regime. It would not be considered personal data, as it would not be likely that the individual could be identified from that dataset. That is a real problem because pseudonymised datasets are very common with large datasets. There are real risks there that would not be dealt with.

Q161 Stephanie Peacock: On average, how long does it currently take for data subjects to resolve basic data rights breaches?

Alex Lawrence-Archer: Under the current regime, that is a bit like asking, "How long is a piece of string?" It can take quite a long time. There are certain practices

that the ICO follows in terms of requiring individuals to complain to the controller first. Some controllers are good; some are quick, but some are not. You might have a lot of back and forth about data access at the beginning, but other controllers might hand over your data really quickly. However, you could be looking at anything up to, say, 10 to 12 months.

Q162 Stephanie Peacock: Do you think that any changes in the Bill, for example those surrounding subject access requests, would increase that time?

Alex Lawrence-Archer: Yes. You have heard from lots of people about the changes to the standard to be applied when any of the rights in chapter 3 are exercised by a data subject, and that includes the right of access. I think it is very likely that many more exercises of the right of access will be refused, at least initially. I think there will be many more complaints about the right of access and there is likely to be satellite litigation about those complaints as well, because you cannot proceed in finding out what has gone on with your data and rectify a problem unless you have access to the copies of it.

So, what you might find in many cases is a two-stage process whereby, first, you must resolve a complaint, maybe even a court case, about your right to access the data and then, and only then, can you figure out what has actually been going on with it and resolve the underlying unlawfulness in the processing. Effectively, therefore, it is a doubling of the process for the individual.

Q163 Stephanie Peacock: A final question: do you think that the definitions of "vexatious" and "excessive" are clear enough not to be abused by controllers who simply do not want to carry out subject access requests?

Alex Lawrence-Archer: The new definitions, particularly the list of factors to be taken into consideration in determining whether the test is met, provide a lot of breathing room for controllers, whether or not they have good intentions, to make arguments that they do not need to comply with the right of access. If you are looking not to comply or if you have an incentive not to, as many controllers do, that does not necessarily mean that you are acting in bad faith; you might just not want to hand over the data and think that you are entitled not to do so. If you are looking not to comply, you will look at the Act and see lots of hooks that you can hang arguments on. Ultimately, that will come back to individuals who are just trying to exercise their rights and who will be engaged in big arguments with big companies and their lawyers.

Q164 Damian Collins: The age-appropriate design code for children was mentioned in our session this morning. Do you have any thoughts on what the Bill could mean for the application of that design code, which was obviously prepared for an environment in which GDPR was enshrined in UK data law?

Alex Lawrence-Archer: The age-appropriate design code was a real success for the UK in terms of its regulation and its reputation internationally. It clarified the rights that children have in relation to the processing of their personal data. However, those rights are only helpful if you know what is happening to your personal data, and if and when you find out that you can exercise your rights in relation to that processing.

As I have said, what the Bill does—again, perhaps inadvertently—is undermine in a whole host of ways your ability to know what is happening with your personal data and to do something about it when you find out that things have gone wrong. It seems to me that on the back of a notable success in relation to the AADC, we are now, with this Bill, moving in rather a different direction in terms of that argument for protection of personal data.

Looking at the even longer term, there will be some slightly more nuanced changes if and when the AADC comes to be amended or redrafted, because of the role of the ICO and the factors that it has to take into account in its independence, which again you have already heard about. So you could, in the long term, see a new version of the AADC that is more business-friendly, potentially, because of this Bill.

Q165 Damian Collins: In terms of access to personal data, a lot of what we are talking about, certainly when we are talking about children, relates to what we generally call big-tech companies. A lot of the age-appropriate design code is focused on children's interface with services like Instagram, YouTube, TikTok and so on, of which they are heavy users. Are you concerned that because data may be stored in such a way that it is difficult for an external person to locate to an individual user, companies may use that as an excuse to be much looser in their application of the protections for children?

Alex Lawrence-Archer: There are a bunch of different ways in which companies will take advantage of the new grey areas that the Bill opens up to carry out processing with less transparency and less respecting of the rights of the people whose data they are processing. If we take just the definition of research, for example, it will be much easier to carry out research for a large platform that already has lots of personal data. The GDPR already provides for a lot of exemptions when you are carrying out research; the Bill dramatically expands that definition. If you are a Google or a YouTube, then yes, you are much freer to carry out processing that you consider to be research without necessarily being transparent about it to the users affected, those whose data it concerns.

Q166 Damian Collins: The project that triggered the initial Cambridge Analytica scandal was in theory academic research on personality profiling, so there are lots of ways in which the definition can be stretched, for sure. Earlier, I asked the Information Commissioner about the definition of legitimate interests for companies. He seemed to think that if he thought that someone did not have a legitimate interest, he could still investigate it and therefore the Bill did not make much difference, but are you reassured by what he said?

Alex Lawrence-Archer: We need to distinguish between two things: one is the introduction of some examples of what may be legitimate interests, which is not a particular concern because they replicate what is already in a recital; and, separately and of much greater concern, the introduction of recognised legitimate interests. I think that that is quite a radical departure from legitimate interests under the current regime. The Bill possibly misguides people, because it uses the language of legitimate interests, but it works in a very different way.

If you have a legitimate interest under the current regime, you must balance your interests against those of data subjects, and that is not something that is required if you can rely on a recognised legitimate interest under the new regime. The recognised legitimate interests are very broad—prevention of crime, for example, does not mean that that has to be done by the police. That is about opening up such processing for any kind of controller, which could be your neighbour or local corner shop, who can rely on that recognised legitimate interest with no requirement to consider the data subject's interest at all. That is a radical departure, because the concept of balancing the interests of the data subject and of the controller is absolutely fundamental to our current regime.

Q167 Damian Collins: In that case, on recognised legitimate interests, if someone says that their legitimate interest is the prevention of crime, they can define that in any way that they like in how they might seek to process or analyse behaviour patterns in their systems?

Alex Lawrence-Archer: I do not want to overstate the case. You must be able to demonstrate that the processing is necessary for a recognised legitimate interest; it has got to make sense—but you do not have to consider anyone else's interests.

For example, in some recent cases, neighbours were operating CCTV that captured lots of the personal data of their neighbours. An important argument to show that that was unlawful was that yes, the processing was necessary for the detection of crime—that is what the CCTV was for—but the interests of the neighbours, views of whose gardens and front windows were being captured, overrode the legitimate interests of the controller. That is how it works under the current regime. Under the new regime, you would not have to consider the interests of the neighbours in the use of that CCTV system. You would be able to rely on the recognised legitimate interest.

Q168 Damian Collins: Effectively, you would not need to consider whether the use of that technology in that case was disproportionate to the risk.

Alex Lawrence-Archer: Yes.

Q169 Chi Onwurah: We heard from some witnesses today that greater ease of access to data will increase competition for those such as Google and Meta that have large amounts of data as it is. What do you think the impact of this Bill will be for big tech?

Alex Lawrence-Archer: I think the Bill is quite big tech-friendly, and the way that it deals with research is well illustrative of that. One of the objectives of the Bill is obviously to boost the use of personal data for academic research, which is a really laudable objective. However, the main change—in fact the only change I can think of off the top of my head—that it makes is to broaden the definition of academic research. That helps people who already have lots of personal data they might do research with; it does not help you if you do not have personal data. That is one of the major barriers for academics at the moment: they cannot get access to the data they need.

The Bill does nothing to incentivise or compel data controllers such as online platforms to actually share data and get it moving around the system for the purposes of academic research. This is in stark contrast to the approach being taken elsewhere. It is an issue the EU is starting to grapple with in a particular domain of research with article 40 of the Digital Services Act. There is a sense that we are falling behind a little bit on that key barrier to academic research with personal data.

Q170 Chi Onwurah: We also heard that existing cookie management and subject access requests and so on represent a real burden, particularly for smaller companies. Do you recognise that? Do you know why there is less support in technology to help small businesses deal with, if you like, the data management challenges? How is that to be traded off against the privacy rights of individuals?

Alex Lawrence-Archer: I certainly recognise that the requirements of GDPR place compliance burdens on businesses of all sizes. I am sceptical that the right balance is being struck in trying to ameliorate the burdens of the costs and challenges that ordinary people will face—in terms of knowing how they are being profiled and tracked by companies—and resolving things when they have gone wrong. I am sceptical as well that there will be major benefits to many businesses who will continue to need to do business in Europe. For that reason, we will need either to have dual compliance or simply to continue to comply with EU GDPR. You can see this benefiting the largest companies, which can start to segment their users. We have already seen that with Meta, which moved its users on to US controllership, for example. I would see that as more beneficial to those large companies, which can navigate that, rather than, say, SMEs.

The Chair: Mr Lawrence-Archer, thank you very much for your time this afternoon.

That brings us to the end of our 11th panel. As an impartial participant in these proceedings—we have had over four-and-a-half hours of evidence with 23 witnesses—I would say it has been an absolute masterclass in all the most topical issues in data protection and digital information. Members might not realise it, but that is what we have had today.

Ordered, That further consideration be now adjourned. *—(Steve Double.)*

4.33 pm

Adjourned till Tuesday 16 May at twenty-five minutes past Nine o'clock.

Written evidence reported to the House

DPDIB01 Judith Ratcliffe, Privacy Professional
DPDIB02 Dr C N M Pounder, Amberhawk Training Limited
DPDIB03 Prighter Ltd
DPDIB04 Damien Welfare
DPDIB05 Data and Marketing Association (DMA)
DPDIB06 Open Rights Group
DPDIB07 Big Brother Watch
DPDIB08 TrueLayer
DPDIB09 Internet Advertising Bureau (IAB) UK

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Third Sitting

Tuesday 16 May 2023

(Morning)

CONTENTS

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 20 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

† Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Eastwood, Mark *(Dewsbury)* (Con)
† Henry, Darren *(Broxtowe)* (Con)
† Hunt, Jane *(Loughborough)* (Con)
† Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Monaghan, Carol *(Glasgow North West)* (SNP)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
† Richards, Nicola *(West Bromwich East)* (Con)
† Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 16 May 2023

(Morning)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

9.25 am

The Chair: I have a few preliminary announcements that Mr Speaker would like me to make. *Hansard* colleagues would be grateful if Members emailed their speaking notes to hansardnotes@parliament.uk. Please switch electronic devices to silent mode. Tea and coffee are not allowed during sittings.

The selection list for today's sitting, which is available in the room, shows how the selected amendments have been grouped for debate. Grouped amendments are generally on the same or a similar issue. Please note that decisions on amendments will take place not in the order in which they are debated, but in the order in which they appear on the amendment paper. The selection and grouping list shows the order of debates. Decisions on each amendment will be taken when we come to the clause to which the amendment relates.

The Member who has put their name to the lead amendment in a group will be called first. Other Members will then be free to catch my eye to speak on all or any of the amendments within that group. A Member may speak more than once in a single debate. At the end of a debate on a group of amendments, I shall again call the Member who moved the lead amendment. Before they sit down, they will need to indicate to me whether they wish to withdraw the amendment or to seek a decision. If any Member wishes to press any other amendment in a group to a vote, they will need to let me know.

Clause 1

Information relating to an identifiable living individual

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

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): It is a pleasure to serve under your chairmanship, Mr Hollobone. May I thank all hon. Members for volunteering to serve on the Committee? When I spoke on Second Reading, I expressed my enthusiastic support for the Bill—just as well, really. I did not necessarily expect to be leading on it in Committee, but I believe it is a very important Bill. It is complex and will require quite a lot of scrutiny, but it will create a framework of real benefit to the UK, by facilitating the exchange of data and allowing us to take the maximum advantage of emerging technologies. I look forward to our debates over the next few days.

Clause 1 will create a test in legislation to help organisations to understand whether the data that they are processing is personal or anonymous. This is important, because personal data is subject to data protection rules but anonymous data is not. If organisations can be confident that the data they are processing is anonymous, they will be able to use it for important activities such as research and product development without concern about the potential impact on individuals' personal data.

The new test will require data controllers considering whether data is personal or anonymous to consider two scenarios. The first is where a living individual can be identified by somebody within the data controller or processor's own organisation using reasonable means at any point at which the data is being processed, from the initial point of collection for its use and storage to its eventual deletion or onward transmission. The second scenario is where the data controller or processor knows or should reasonably know that somebody outside the organisation is likely to obtain the information and to be able to re-identify individuals from it using reasonable means. That could be a research partner or a business client with whom the data controller intends to share the data, or an outside organisation that obtains the data as a result of the data controller not putting adequate security measures in place.

What would be considered "reasonable means" in any given case takes into account, among other things, the time, effort and cost of identifying the individual, as well as the technology available during the time the processing occurs. We hope that the clarity the test provides will give organisations greater confidence about using anonymous data for a range of purposes, from marketing to medical research. I commend the clause to the Committee.

Stephanie Peacock (Barnsley East) (Lab): It is a pleasure to serve under your chairship, Mr Hollobone. I echo the Minister's thanks to everyone serving on the Bill Committee; it is indeed a privilege to be here representing His Majesty's loyal Opposition. I look forward to doing our constitutional duty as we scrutinise the Bill today and in the coming sittings.

The definition of personal data is critical, not only to this entire piece of legislation, but to the data protection regime more widely. That is because the definition of what counts as personal data sets the parameters on who will benefit from protections and safeguards set out by the legislation, and, looking at it from the other side, the various protections will not apply when data is not classed as personal. It is therefore important that the definition should be clear for both controllers and data subjects, so that everyone understands where regulations and, by extension, rights do and do not apply.

The Bill defines personal data as that where a data subject can be identified by a controller or processor, or anyone likely to obtain the information,

"by reasonable means at the time of processing".

According to the Bill, "reasonable means" take into account the time, effort, costs, technology and resources available to the person. The addition of "reasonable" to the definition has caused major concern among civil society groups, which are worried that it will introduce an element of subjectivity from the perspective of the controller when determining whether data is personal or not. Indeed, although recital 26 of the General Data Protection Regulation also refers to reasonable means—making this, in some ways, more of a formal change

than a practical one—there must still be clear parameters on how controllers or processors are to make that judgment. Without those, there may be a danger of controllers and processors avoiding the requirement to comply with rules around personal data by simply claiming they do not have the means to identify living individuals within their resources.

Has the Department undertaken an impact assessment to determine whether the definition could, first, increase subjectivity in what counts as personal data, or secondly, reduce the amount of data classified as personal data? If an assessment identifies such a risk, what steps will the Department take to mitigate that and ensure that citizens are able to exercise their rights as they can under the current definition?

Other stakeholders have raised concerns that the phrase

"at the time of the processing"

in the definition might imply that there is no continuous obligation to consider whether data is personal. Indeed, under the current definition, where personal data is

"any information that relates to an identified or identifiable living individual",

there is an implied obligation to consider whether an individual is identifiable on an ongoing basis. Rather than assessing the identifiability of a dataset at a fixed point, the controller or processor must keep the categorisation of data that it holds under careful review, taking into account technological developments, such as sophisticated new artificial intelligence or cross-referencing tools. Inserting the phrase

"at the time of the processing"

into this definition has prompted the likes of Which? to express concern that some processors may feel that they are no longer bound by this continuous obligation. That would be particularly worrying given the potential subjectivity of the new definition. If whether an individual is identifiable is based on "reasonable means", including one's resources and technology, it is perfectly feasible that, with a change of resources or technology, it could become reasonable to identify a person when once it was not.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): My hon. Friend is making an excellent speech. Does she agree that the absence of regard for the rate of technological change, particularly the rise of artificial intelligence—datasets are now being processed at phenomenal speeds—is potentially negligent on the part of the Government?

Stephanie Peacock: My hon. Friend makes an important point, which I will come to later.

In these circumstances, it is crucial that if a person is identifiable through data at any time in the future, the data is legally treated as personal so that the relevant safeguards and rights that GDPR was designed to ensure still apply.

When arguing for increased Secretary of State powers across the Bill, Ministers have frequently cited the need to future-proof the legislation. Given that, we must also consider the need to future-proof the definition of data so that technological advances do not render it useless. Does the new definition involve a continuous obligation to assess whether data is personal? Will guidance be offered to inform both controllers and data subjects on the application of this definition, so that both sides can be clear on how it will work in practice? As 5Rights has pointed out, that could avoid clogging up the regulator's time with claims about what counts as personal data in many individual cases.

Finally, when determining whether data is personal, it is also vital that controllers take into account how a determined stalker or malicious actor might find and use their data. It is therefore good to see the change made since the first iteration of the Data Protection and Digital Information Bill, to clarify that

"obtaining the information as a result of the processing"

also includes information obtained as a result of inaction by a controller or processor—for example, as the result of a failure to put in place appropriate measures to prevent or reduce the risk of hacking.

Overall, it is important that we give both controllers and data subjects clarity about which data is covered by which protections, and when. I look forward to hearing from the Minister about the concerns that have been raised, which could affect the definition's ability to allow for that clarity.

Sir John Whittingdale: I agree absolutely with the hon. Lady that the definition of personal data is central to the regime that we are putting in place. She is absolutely right that we need to be very clear and to provide organisations with clarity about what is within the definition of personal data and what is rightly considered to be anonymous. She asks whether the provision will lead to a reduction in the current level of protection. We do not believe that it will.

Clause 1 builds on the strong foundations used in GDPR recital 26 to clarify when data can be categorised as truly anonymous without creating undue risks. The aim of the provision in the Bill is to clarify when information should be considered to be personal data by including a test for identifiability in the legislation. That improved clarity will help organisations to determine when data can be considered truly anonymous and therefore pose almost no risk to the data subject.

The hon. Lady asked whether

"at the time of the processing"

extends into the future, and the answer is yes. The definition of data processing in the legislation is very broad and includes a lot of processing activities other than just the collection of data, such as alteration, retrieval, storage and disclosure by transmission, to name just a few. The phrase

"at the time of the processing"

could therefore cover a long period, depending on the nature and purpose of the processing. The test would need to be applied afresh for each new act of processing. That means that if at any point in the life cycle of processing, the data could be reasonably re-identified by someone by reasonable means, they would then not be able to legally consider to be anonymous. That includes transferring abroad to other regimes.

The clause makes it clear that a controller will have to consider the likelihood of re-identification at all stages of the processing activity. If a data controller held a dataset for several years, they would need to be mindful of the technologies available during that time that might be used to re-identify it. As the hon. Lady said, technology is advancing very fast and could well change over time from the point at which the data is first collected.

Chi Onwurah: I appreciate the Minister's clarification. He has just said that the test of identification would apply when sharing the data with another authority. However, once that has been done, the test no longer applies. Does he accept that it is possible for data to be shared that could not by this test reasonably be identified but that, over time, in a different authority, could reasonably be identified, without the data subject having any redress?

Sir John Whittingdale: If data is shared and then held by a new controller, it will be still subject to the same protections even though it has been transferred from the original. It is important that there should be the ability to continue to apply protection no matter what technology evolves over the course of time, but it will still be subject to the same protection and, of course, still be enforceable through the Information Commissioner.

Chi Onwurah: Would it be subject to the same protection if it was transferred abroad?

Sir John Whittingdale: Again, yes, it will. It will be transferred abroad only if we are satisfied that the recipient will impose the same level of protection that we regard as necessary in this country.

Question put and agreed to.

Clause 1 accordingly ordered to stand part of the Bill.

Clause 2

MEANING OF RESEARCH AND STATISTICAL PURPOSES

Stephanie Peacock: I beg to move amendment 66, clause 2, page 4, line 8, at end insert—

"(c) do not include processing of personal data relating to children for research carried out as a commercial activity."

This amendment would exempt children's data from being used for commercial purposes under the definition of scientific purposes in this clause.

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

Amendment 65, clause 2, page 4, line 21, at end insert—

"7. The Commissioner must prepare a code of practice under section 124A of the Data Protection Act 2018 on the interpretation of references in this Regulation to "scientific research".

8. The code of practice prepared under paragraph 7 must include examples of the kinds of research purposes, fields, controllers, and ethical standards that are to be considered as being scientific, and those that are excluded from being so considered."

This amendment would require a statutory code of practice from the ICO on how the definition of scientific research in this clause is to be interpreted.

Clause stand part.

Stephanie Peacock: Fuelling safe scientific research through data will be vital to support the UK's ambition to become a science superpower. We understand that, as is the case in many areas of data protection law, lack of clarity about what counts as processing for scientific purposes causes organisations to take a risk-averse approach to conducting research. An understanding of exactly what is included would therefore give organisations confidence they need to conduct vital processing that will allow for the scientific discoveries and benefits of the future.

Unfortunately, the clause makes the same mistake as the Bill does in general by focusing on easing regulations on those who hold data, rather than looking at how data can be harnessed for the general greater good. It misses the opportunity to unlock the benefits of safely redistributing and sharing data. Indeed, none of the clauses on processing for research purposes make any attempt to explore options to incentivise controllers to share their data with independent researchers. Similarly, the Bill does not explore how the likes of data trusts or co-operatives that pool data resources in the interests of a larger group of beneficiaries or organisations could create a stronger environment for research. Instead, it leaves those who already collect and hold data to benefit from the regime by processing for their own research purposes, while those who might hope to collaborate will use alternative data sets and are no better off.

By failing to think about the safe sharing of data to fuel scientific research, the Government limit the progress the UK could make as a powerhouse of science innovation. The Bill leaves only those organisations with large amounts of data able to contribute to such progress, entrenching existing power structures and neglecting the talent held in the smaller independent organisations that would otherwise be able to conduct research for the public good.

Turning to amendment 65, it has always been written into the GDPR, in recital 159, that processing for scientific purposes should be interpreted broadly. It is therefore understandable why Ministers provided a broad definition in the Bill that allows for those conducting genuine scientific research to have absolute confidence that their processing falls under this umbrella, preventing a risk-averse environment. However, stakeholders, including Reset.tech and the Ada Lovelace Institute, have expressed worries that clause 2 goes a little too far, essentially providing a blank cheque for private companies to self-identify as conducting scientific research as a guise for processing personal information for any purpose they choose.

All that must be understood in combination with clause 9, which gives organisations an exemption from purpose limitation, allowing them to reuse data as long as it is for scientific purposes, as defined in clause 2. Indeed, though the Bill contains a few clarifications of what the definition in clause 2 includes, such as publicly and privately funded processing, commercial or non-commercial processing and processing for the likes of technological development, fundamental research, or applied research, I am keen to hear from the Minister about what specific purposes would actually be ruled out under the letter of the current definition. For example, as the Ada Lovelace Institute asked, would pseudoscientific applications, such as polygraphy or experimental AI claiming to predict an individual's religion, politics or sexuality, be categorically ruled out under the current definition?

Though it may not be the intention in the clause to enable malicious or pseudoscientific processing under the definition of science, we must ensure that the definition is not open to exploitation, or so broad that any controller could reasonably identify their processing as falling under it. Regulator guidance would be in a prime position to do that. By providing context as to what must be considered for something to be reasonably classified as scientific—for example, the purpose of the research, the

field of research, the type of controller carrying it out, or the methodological and ethical standards used—controllers using the definition legitimately will feel even more assured, and malicious processing will be explicitly excluded from the application of the definition. Amendment 65 would do nothing to stop genuinely scientific research from benefiting from the changes in this Bill and would provide further clarity around how the definition can be legitimately relied upon.

9.45 am

Turning to amendment 66, 5Rights is a leading non-governmental, non-profit charitable organisation that seeks to reimagine the digital world in a way that works for children. Like others, it has shared concerns that relaxing the legal bases on which personal data can be processed for scientific research to include privately funded research carried out by commercial entities could open the door for children's data to be exploited for commercial purposes. Clause 9 will change rules to allow processors to not inform data subjects about the reuse of their data so long as it is for scientific purposes, even if that is on a commercial basis.

Even under the existing regulatory framework, there have been plenty of examples where controllers have claimed to be using data in the best interests of young people while actually causing them harm. The development of educational technology is widely cited as the future of education, with the industry rapidly expanding because of online learning during the pandemic. However, although such technologies and services claim to be for the benefit of children, many have used children's data in irresponsible ways.

A 2022 report by Human Rights Watch reviewed 165 ed tech products endorsed by 49 Governments worldwide that were deployed in schools and colleges during the lockdowns. The study found that 89% of the products engaged in data practices that put children's rights at risk, undermined them or actively violated them. Companies monitored children without their consent or knowledge and harvested data on what they do, who they are, where they live or study and who their family and friends are to the extent that the report concluded that the only way for children to protect themselves from the invasion would be to throw their devices in the trash.

The majority of learning platforms also sent or allowed advertising technology companies to access children's data. These ad tech companies, many of which are owned by the most powerful companies in the world, can then analyse and profile children, piecing the information together with data from other public or private sources to create detailed profiles that are used to place targeted adverts or can be sold to advertisers. From that study and others like it we can clearly see that even under the current rules children's data is vulnerable to being exploited for commercial gain. It would therefore be a great mistake to make the processing of children's data for commercial purposes even less transparent than it already is.

As was the aim with the age appropriate design code, it is important that we give children a high level of privacy rights by default. Where children's data is concerned, extra safeguards must be in place to ensure that any processing that occurs is in their best interests. Amendment 66 seeks to set an example of such a safeguard in practice, providing an exemption for children's data from being defined as scientific where it is being used for commercial purposes. It will hopefully create a precedent whereby children's rights are automatically given the best protection possible.

I would like to finish by asking the Minister whether his Department has considered the impact of the new legislation on commercial scientific processing on children specifically. If so, what measures have been taken to ensure that the Bill does not put children's personal data at risk of exploitation?

Damian Collins (Folkestone and Hythe) (Con): I wish to pose a couple of questions, after two thoughtful and well-presented amendments from those on the Opposition Front Bench. With regard to children and the use of apps such as TikTok, what assurance will the Government seek to ensure that companies that process and store data abroad are abiding by the principles of our domestic legislation? I mention TikTok directly because it stores data from UK users, including children, in Singapore, and it has made clear in evidence to the Joint Committee on the Online Safety Bill that that data is accessed by engineers in China who are working on it.

We all know that when data is taken from a store and used for product development, it can be returned in its original state but a huge amount of information is gathered and inferred from it that is then in the hands of engineers and product developers working in countries such as China and under very different jurisdictions. I am interested to know what approach we would take to companies that store data in a country where we feel we have a data equivalence regime but then process the data from a third location where we do not have such a data agreement.

Sir John Whittingdale: I welcome the recognition of the importance of allowing genuine research and the benefits that can flow from it. Such research may well be dependent on using data and the clause is intended to provide clarity as to exactly how that can be done and in what circumstances.

I will address the amendments immediately. I am grateful to the hon. Member for Barnsley East for setting out her arguments and we understand her concerns. However, I think that the amendments go beyond what the clause proposes and, in addition, I do not think that there is a foundation for those concerns. As we have set out, clause 2 inserts in legislation a definition for processing for scientific research, historical research and statistical purposes. The definition of scientific research purposes is set out as

"any research that can be reasonably described as scientific"

and I am not sure that some of the examples that the hon. Lady gave would meet that definition.

The definitions inserted by the clause are based on the wording in the recitals to the UK GDPR. We are not changing the scope of these definitions, only their status in the legislation. They will already be very familiar to people using them, but setting them out in the Bill will provide more clarity and legal certainty. We have maintained a broad scope as to what is allowed to be included in scientific research, with the view that the regulator can add more nuance and context through guidance, as is currently the case. The power to require codes of practice provides a route for the Secretary of State to require the Information Commissioner to prepare any code of practice that gives guidance on good practice in processing personal data.

[Sir John Whittingdale]

There will be situations where non-statutory guidance, which can be produced without being requested under regulations made by the Secretary of State, may be more appropriate than a statutory code of practice. Examples of the types of activity that are considered scientific research and the indicative criteria that a researcher should demonstrate are best placed in non-statutory guidance produced by the Information Commissioner's Office. That will give flexibility to amend and change the examples when necessary, so I believe that the process does not change the provision. However, putting it in the legislation, rather than in the recitals, will impose stronger safeguards and make things clearer. Once the Bill has come into effect, the Government will continue to work with the ICO to update its already detailed and helpful guidance on the definition of scientific research as necessary.

Amendment 66 would prohibit the use of children's data for commercial purposes under the definition of scientific research. The definition inserted by clause 2 includes the clarification that processing for scientific research carried out as a commercial activity can be considered processing for scientific research purposes. Parts of the research community asked for that clarification in response to our consultation. It reflects the existing scope, as is already clear from the ICO's guidance, and we have seen that research by commercial bodies can have immense societal value. For instance, research into vaccines and life-saving treatments is clearly in the public interest. I entirely understand the hon. Lady's concern for children's privacy, but we think that her amendment could obstruct important research by commercial organisations, such as research into children's diseases. I think that the Information Commissioner would make it clear as to whether or not the kind of example that the hon. Lady gave would fall within the definition of research for scientific purposes.

I also entirely understand the concern expressed by my hon. Friend the Member for Folkestone and Hythe. I suspect that the question about the sharing of data internationally, particularly, perhaps, by TikTok, may recur during the course of our debates. As he knows, we would share data internationally only if we were confident that it would still be protected in the same way that it is here, which would include considering the possibility of whether or not it could then be passed on to a third country, such as China.

I hope that I can reassure the hon. Lady that emphasising the safeguards that researchers must comply with in clause 22 to protect individuals relates to all data used for these purposes, including children's data and the protections afforded to children under the UK GDPR. For those reasons, I hope that she will be willing to withdraw her amendment.

Stephanie Peacock: I am disappointed that the Minister does not accept amendment 66. Let me make a couple of brief points about amendment 65. The Minister said that he was not sure whether some of the examples I gave fitted under the definition, and that is what the amendment speaks to. I asked what specific purposes would be ruled out under the letter of the current definition, and that is still not clear, so I will press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 1]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Amendment proposed: 65, in clause 2, page 4, line 21, at end insert—

"7. The Commissioner must prepare a code of practice under section 124A of the Data Protection Act 2018 on the interpretation of references in this Regulation to 'scientific research'.

8. The code of practice prepared under paragraph 7 must include examples of the kinds of research purposes, fields, controllers, and ethical standards that are to be considered as being scientific, and those that are excluded from being so considered."—*(Stephanie Peacock.)*

This amendment would require a statutory code of practice from the ICO on how the definition of scientific research in this clause is to be interpreted.

The Committee divided: Ayes 6, Noes 9.

Division No. 2]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Clause 2 ordered to stand part of the Bill.

Clause 3

CONSENT TO PROCESSING FOR THE PURPOSES OF SCIENTIFIC RESEARCH

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

The Chair: With this it will be convenient to discuss clause 4 stand part.

Sir John Whittingdale: The clause clarifies how the conditions for consent will be met in certain circumstances when processing for scientific research purposes. It clarifies an existing concept of "broad consent" that is currently found in the recitals. The measure will enable consent to

be obtained for an area of scientific research when the researcher cannot fully identify the purposes for which they are collecting the data.

Consent under UK GDPR must be for a specific purpose, but in scientific research the precise purpose may not be fully known when the data is collected. For example, the initial aim may be the study of cancer, and then later becomes the study of a particular cancer type. Currently, the UK GDPR recitals clarify that consent may be given for an area of scientific research, but as the recitals are only an interpretative aid that may not give scientists the certainty that they need. The clause will therefore add the ability to give broad consent for scientific research into the operative text of the UK GDPR, giving scientists greater certainty and confidence. The clause contains a number of safeguards to protect against misuse. That includes the requirement that seeking consent is consistent with ethical standards that are generally recognised and relevant to that area of research.

10 am

Although law enforcement agencies have the power to process personal data with the permission of the individual, there is no definition of consent in the legislation. Clause 4 again mirrors the UK GDPR definition of consent, including the conditions that must be met in order for it to be used as a lawful basis for processing. That change will address the slight risk that consent may be interpreted inconsistently with the definition used in the UK GDPR. We are taking this opportunity to make our data protection laws more consistent, by clarifying terminology for both organisations and individuals. I therefore commend the clauses to the Committee.

Stephanie Peacock: With regard to clause 3, I refer Members to my remarks on clause 2. It is sensible to clarify how controllers and processors conducting scientific research can gain consent where it is not possible to fully identify the full set of uses for that data when it is collected. However, what counts as scientific, and therefore what is covered by the clause, must be properly understood by both data subjects and controllers through proper guidance issued by the ICO.

Clause 4 is largely technical and inserts the recognised definition of consent into part 3 of the Data Protection Act 2018, for use when it is inappropriate to use one of the law enforcement purposes. I will talk about law enforcement processing in more detail when we consider clauses 16, 24 and 26, but I have no problem with the definition in clause 4 and am happy to accept it.

Sir John Whittingdale: I am grateful to the hon. Lady for her support. I agree with her on the importance of ensuring that the definition of scientific research is clear. That is something on which I have no doubt the ICO will also issue guidance.

Question put and agreed to.

Clause 3 accordingly ordered to stand part of the Bill.

Clause 4 ordered to stand part of the Bill.

Clause 5

LAWFULNESS OF PROCESSING

Stephanie Peacock: I beg to move amendment 68, in clause 5, page 6, line 37, at end insert—

"7A. The Secretary of State may not make regulations under paragraph 6 unless—

(a) following consultation with such persons as the Secretary of State considers appropriate, the Secretary of State has published an assessment of the impact of the change to be made by the regulations on the rights and freedoms of data and decision subjects (with particular reference to children),

(b) the Commissioner has reviewed the Secretary of State's statement and published a statement of the Commissioner's views on whether the change should be made, with reasons, and

(c) the Secretary of State has considered whether to proceed with the change in the light of the Commissioner's statement."

This amendment would make the Secretary of State's ability to amend the conditions in Annex 1 which define "legitimate interests" subject to a requirement for consultation with interested parties and with the Information Commissioner, who would be required to publish their views on any proposed change.

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

Amendment 67, in clause 5, page 7, line 18, at end insert—

"11. Processing may not be carried out in reliance on paragraph 1(ea) unless the controller has published a statement of—

(a) which of the conditions in Annex 1 has been met which makes the processing necessary,

(b) what processing will be carried out in reliance on that condition, or those conditions, and

(c) why that processing is proportionate to and necessary for the purpose or purposes indicated in the condition or conditions."

This amendment would require controllers to document and publish (e.g. in a privacy notice) a short statement on their reliance on a "recognised legitimate interest" for processing personal data.

Clause stand part.

Stephanie Peacock: At present, the lawful bases for processing are set out in article 6 of the UK GDPR. At least one of them must apply whenever someone processes personal data. They are consent, contract, legal obligation, vital interests, public task, and legitimate interests. That is where data is being used in ways that we would reasonably expect, there is minimal privacy impact, or there is a compelling justification for processing. Of the existing lawful bases, consent is by far the most relied upon, as it is the most clear. There have therefore been calls for the other lawful bases to be made clearer and easier to use. It is welcome to see some examples of how organisations might rely on the legitimate interests lawful ground brought on to the statute book.

At the moment, in order to qualify for using legitimate interests as grounds for lawful processing, a controller must also complete a balancing test. The balancing test is an important safeguard. As per the ICO, it requires controllers to consider the interests and fundamental rights and freedoms of the individual, and whether they override the legitimate interests that the controller has identified. That means at a minimum considering the nature of the personal data being processed, the reasonable expectations of the individual, the likely impact of processing on the individual, and whether any safeguards can be put in place to mitigate any negative impacts.

[Stephanie Peacock]

As tech.UK mentioned, the introduction of a list of legitimate interests no longer requiring that test is something many have long called for. When conducting processing relating to an emergency, for example, the outcome of a balancing test often very obviously weighs in one direction, making the decision straightforward, and the test itself an administrative task that may slow processing down. It makes sense in such instances that a considered exemption might apply.

However, given the reduction in protection and control for consumers when removing a balancing test, it is vital that a list of exemptions is limited and exhaustive, and that every item on such a list is well consulted on. It is also vital that the new lawful basis cannot be relied upon in bad faith or exploited by those who simply want to process without the burden, for reasons outside of those listed in annex 1. The Bill as it currently stands does not do enough to ensure either of those things, particularly given the Secretary of State's ability to add to the list on a whim.

I turn to amendment 67. Although it is likely not the intention for the clause to be open to exploitation, Reset.tech, among many others, has shared concerns that controllers may be able to abuse the new lawful basis of "recognised legitimate interests", stretching the listed items in annex 1 to cover some or all of their processing, and giving themselves flexibility over a wide range of processing without an explicit requirement to consider how that processing affects the rights of data and decision subjects. That is particularly concerning where controllers may be able to conflate different elements of their processing.

Reset.tech and AWO provide a theoretical case study to demonstrate that point. Let us say that there is a gig economy food delivery company that processes a range of data on workers, including minute-by-minute location data. That location data would be used primarily for performance management, but could occasionally be used in more extreme circumstances to detect crime—for example, detecting fraud by workers who are making false claims about how long they waited for an order to be ready for delivery. By exploiting the new recognised legitimate interests basis, the company could conflate its purposes of performance management and detecting crime, and justify the tracking of location data as a whole as being exempt from the balancing test, without having to record or specify exactly which processing is for the detection of crime.

Under the current regime, there remain two tests other than the balancing test that form a complete assessment of legitimate interests and help to prevent conflation of that kind. First, there is the purpose test, which requires the controller to identify which legitimate interest the company is relying upon. Secondly, there is the necessity test, which requires the controller to consider whether the processing that the company intends to conduct is necessary and proportionate to meet its purposes.

In having to conduct those tests, the food delivery company would find it much more difficult to conflate its performance management and crime prevention purposes, as it would have to identify and publicly state exactly which elements of its processing are covered by the legitimate interest purpose of crime prevention. That would make it explicit that any processing the company conducts for the purposes of performance management is not permitted under a recognised legitimate interest, meaning that a lawful basis for that processing would be required separately.

Amendment 67 therefore seeks to ensure that the benefits of the purpose and necessity tests are retained, safeguarding the recognised legitimate interests list from being used to cynically conflate purposes and being exploited more generally. In practice, that would mean that controllers relying on a purpose listed in annex 1 for processing would be required to document and publish a notice that explains exactly which processing the company is conducting under which purpose, and why it is necessary.

It is foundational to the GDPR regime that each act of processing has a purpose, so this requirement should just be formalising and publishing what controllers are already required to consider. The measure that the amendment seeks to introduce should therefore be no extra burden on those already complying in good faith, but should still act as a barrier to those attempting to abuse the new basis.

I turn to amendment 68. As the likes of Which? have argued, any instance of removing the balancing test will inevitably enable controllers to prioritise their interests in processing over the impact on data subjects, resulting in weaker protections for data subjects and weaker consumer control. Which? research, such as that outlined in its report "Control, Alt or Delete? The future of consumer data", also shows that consumers value control over how their data is collected and used, and that they desire more transparency, rather than less, on how their data is used.

With those two things in mind—the value people place on control of their data and the degradation of that control as a result of removing the balancing test—it is vital that the power to remove the balancing test is used extremely sparingly on carefully considered, limited purposes only. Even for those purposes already included in annex 1, it is unclear exactly what impact assessment took place to ensure that the dangers of removing the test on the rights of citizens did not outweigh the positives of that removal.

It would therefore be helpful if the Minister could outline the assessment and analysis that took place before deciding the items on the list. Although it is sensible to future-proof the list and amend it as needs require, this does not necessarily mean vesting the power to do so in the Secretary of State's hands, especially when such a power is open to potential abuse. Indeed, to say that the Secretary of State must have regard to the interests and fundamental rights and freedoms of data subjects and children when making amendments to the list is simply not a robust enough protection for citizens. Our laws should not rely on the good nature of the Secretary of State; they must be comprehensive enough to protect us if Ministers begin to act in bad faith.

Further, secondary legislation simply does not offer the scrutiny that the Government claim it does, because it is rarely voted on. Even when it is, if the Government of the day have a majority, defeating such a vote is incredibly rare. For the method of changing the list to be protected from the whims of a bad faith Secretary of State who simply claims to have had regard to people's

rights, proper consultation should be undertaken by the regulator on any amendments before they are considered for parliamentary approval.

This amendment would move the responsibility for judging the impact of changes away from the Secretary of State and place it with the regulator on a yearly basis, ensuring that amendments proceed only if they are deemed, after consultation, to be in the collective societal interest. That means there will be independent assurance that any amendments are not politically or maliciously motivated. This safeguard should not be of concern to anyone prepared to act in good faith, particularly the current Secretary of State, as it would not prevent the progression in Parliament of any amendments that serve the common good. The amendment represents what genuine future-proofing in a way that retains appropriate safeguards looks like, as opposed to what ends up looking like little more than an excuse for a sweeping power grab.

Sir John Whittingdale: I welcome the hon. Lady's recognition of the value of setting out a list of legitimate interests to provide clarity, but I think she twice referred to the possibility of the Secretary of State adding to it on a whim. I do not think we would recognise that as a possibility. There is an established procedure, which I would like to go through in responding to the hon. Lady's concerns. As she knows, one of the key principles of our data protection legislation is that any processing of personal data must be lawful. Processing will be lawful where an individual has given his or her consent, or where another specified lawful ground in article 6 of the UK GDPR applies. This includes where the processing is necessary for legitimate interests pursued by the data controller, providing that those interests are not outweighed by an individual's privacy rights.

Clause 5 addresses the concerns that have been raised by some organisations about the difficulties in relying on the "legitimate interests" lawful ground, which is used mainly by commercial organisations and other non-public bodies. In order to rely on it, the data controller must identify what their interest is, show that the processing is necessary for their purposes and balance their interests against the privacy right of the data subject. If the rights of the data subject outweigh the interests of the organisation, the processing would not be lawful and the controller would need to identify a different lawful ground. Regulatory guidance strongly recommends that controllers document the outcome of their legitimate interests assessments.

As we have heard, and as the hon. Lady recognises, some organisations have struggled with the part of the legitimate interests assessment that requires them to balance their interests against the rights of individuals, and concern about getting the balancing test wrong—and about regulatory action that might follow as a result—can cause risk aversion. In the worst-case scenario, that could lead to crucial information in the interests of an individual or the public—for example, about safeguarding concerns—not being shared by third-sector and private-sector organisations. That is why we are taking steps in clause 5 and schedule 1 to remove the need to do the balancing test in relation to a narrow range of recognised legitimate activities that are carried out by non-public bodies. Those activities include processing, which is necessary for the purposes of safeguarding national security or defence; responding to emergencies; preventing crimes such as fraud or money laundering; safeguarding vulnerable individuals; and engaging with the public for the purposes of democratic engagement.

10.15 am

Amendment 68, tabled by the hon. Member for Barnsley East, would prevent the Secretary of State from using the regulation-making powers in the clause to add to the list of activities for which no balancing test is required unless she has first published an assessment of the impact of the change on the rights of individuals and formally considered any views of the Information Commissioner. The amendment is unnecessary because, as drafted, the clause already requires the Secretary of State to consider the impact of any changes to the list of the rights and freedoms of individuals and, where relevant, the need to provide children with special protection with regard to their personal data.

The regulation-making powers in the clause will also be subject to the new requirements in clause 44. They provide that any regulations made under the UK GDPR are subject to consultation with the commissioner and such other persons as the Secretary of State considers appropriate.

Damian Collins: Will my right hon. Friend confirm whether the Information Commissioner's advice will be published, either by the commissioner, the Minister or Parliament—perhaps through the relevant Select Committee?

Sir John Whittingdale: I am not sure it would necessarily be published. I want to confirm that, but I am happy to give a clear response to the Committee in due course if my hon. Friend will allow me.

As well as the advice that the Information Commissioner supplies, the proposal is also subject to the affirmative procedure, as the hon. Member for Barnsley East recognised, so Parliament could refuse to approve any additions to the list that do not respect the rights of data subjects. She suggested that it is rare for an affirmative resolution to be rejected by Parliament; nevertheless, it is part of our democratic proceedings, and every member of the Committee considering it will have the opportunity to reach their own view and vote accordingly. I hope that reassures the hon. Lady that there are already adequate safeguards in place in relation to the exercise of powers to add new activities to the list of recognised legitimate interests.

Amendment 67, which the hon. Lady also tabled, would require data controllers to publish a statement if they are relying on the new recognised legitimate interests lawful ground. The statement would have to explain what processing would be carried out in reliance on the new lawful ground and why the processing is proportionate and necessary for the intended purpose. In our view, the amendment would significantly weaken the clause. It would reintroduce something similar to the legitimate interests assessment, which, as we have heard, can unnecessarily delay some very important processing activities. In scenarios involving national security or child protection, for example, the whole point of the clause is to make sure that relevant and necessary personal data can be shared without hesitation to protect vulnerable individuals or society more generally.

I hope the hon. Lady is reassured by my response and agrees to withdraw her amendments. I commend clause 5 to the Committee.

Stephanie Peacock: We do not believe that amendment 67 would place an extra burden on those who are already complying in good faith. The idea behind it is that it will be a barrier to those attempting to abuse the new basis.

On amendment 68, we should not have laws that rely on the Secretary of State's good faith. As the Minister said, it is pretty rare for secondary legislation to be voted on, and for the Government to lose, so I do not see that as a barrier. The hon. Member for Folkestone and Hythe highlighted that although there are some protections, we do not believe that the Government protections go as far as we would like. For that reason, I will press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 3]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Amendment proposed: 67, in clause 5, page 7, line 18, at end insert—

"11. Processing may not be carried out in reliance on paragraph 1(ea) unless the controller has published a statement of—

(a) which of the conditions in Annex 1 has been met which makes the processing necessary,

(b) what processing will be carried out in reliance on that condition, or those conditions, and

(c) why that processing is proportionate to and necessary for the purpose or purposes indicated in the condition or conditions.*"—(Stephanie Peacock.)*

This amendment would require controllers to document and publish (e.g. in a privacy notice) a short statement on their reliance on a "recognised legitimate interest" for processing personal data.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 4]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Clause 5 ordered to stand part of the Bill.

Schedule 1

LAWFULNESS OF PROCESSING: RECOGNISED LEGITIMATE INTERESTS

Sir John Whittingdale: I beg to move amendment 30, in schedule 1, page 137, line 28, leave out "fourth day after" and insert

"period of 30 days beginning with the day after".

Annex 1 to the UK GDPR makes provision about processing for democratic engagement purposes, including certain processing by elected representatives. This amendment increases the period for which former members of the Westminster Parliament and the devolved legislatures continue to be treated as "elected representatives" following an election. See also NC6 and Amendment 31.

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

Government amendment 31.

Government new clause 6—*Special categories of personal data: elected representatives responding to requests.*

That schedule 1 be the First schedule to the Bill.

Sir John Whittingdale: As the Committee will be aware, data protection legislation prohibits the use of "special category" data—namely, information about a person that is sensitive in nature—unless certain conditions or exemptions apply. One such exemption is where processing is necessary on grounds of substantial public interest.

Schedule 1 to the Data Protection Act 2018 sets out a number of situations where processing would be permitted on grounds of substantial public interest, subject to certain conditions and safeguards. That includes processing by elected representatives who are acting with the authority of their constituents for the purposes of progressing their casework. The current exemption applies to former Members of the Westminster and devolved Parliaments for four days after a general election—for example, if the MP has been defeated or decides to stand down. That permits them to continue to rely on the exemption for a short time after the election to conclude their parliamentary casework or hand it over to the incoming MP. In practice, however, it can take much longer than that to conclude these matters.

New clause 6 will therefore extend what is sometimes known as the four-day rule to 30 days, which will give outgoing MPs and their colleagues in the devolved Parliaments more time to conclude casework. That could include handing over live cases to the new representative, or considering what records should be retained, stored and deleted. When MPs leave office, there is an onus on them to conclude their casework in a timely manner. However, the sheer volume of their caseload, on top of the other work that needs to be done when leaving office, means that four days is just not enough to conclude all relevant business. The new clause will therefore avoid the unwelcome situation where an outgoing MP who is doing his or her best to conclude constituency casework could be acting unlawfully if they continue to process their constituents' sensitive data after the four-day time limit has elapsed. Extending the time limit to 30 days will provide a pragmatic solution to help outgoing MPs while ensuring the exemptions cannot be relied on for an indefinite period.

Government amendments 30 and 31 will make identical changes to other parts of the Bill that rely on the same definition of "elected representative". Government amendment 30 will change the definition of "elected representative" when the term appears in schedule 1. As I mentioned when we debated the previous group of amendments, clause 5 and schedule 1 to the Bill create a new lawful ground for processing non-sensitive personal data, where the processing is necessary for a "recognised legitimate interest". The processing of personal data by elected representatives for the purposes of democratic engagement is listed as such an interest, along with other processing activities of high public importance, such as crime prevention, safeguarding children, protecting national security and responding to emergencies.

Government amendment 31 will make a similar change to the definition of "elected representative" when the term is used in clause 84. Clauses 83 and 84 give the Secretary of State the power to make regulations to exempt elected representatives from some or all of the direct marketing rules in the Privacy and Electronic Communications (EC Directive) Regulations 2003. I have no doubt that we will debate the merits of those clauses in more detail later in Committee, but for now it makes sense to ensure that there is a single definition of "elected representative" wherever it appears in the Bill. I hope the hon. Member for Barnsley East and other colleagues will agree that those are sensible suggestions and will support the amendments.

Stephanie Peacock: This set of Government provisions will increase the period for which former MPs and elected representatives in the devolved regions can use the democratic engagement purpose for processing. On the face of it, that seems like a sensible provision that allows for a transition period so that data can be deleted, processed, or moved on legally and safely after an election, and the Opposition have a huge amount of sympathy for it.

I will briefly put on record a couple of questions and concerns. The likes of the Ada Lovelace Institute have raised concerns about the inclusion of democratic engagement purposes in schedule 1. They are worried, particularly with the Cambridge Analytica scandal still fresh in people's minds, that allowing politicians and elected parties to process data for fundraising and marketing without a proper balancing test could result in personal data being abused for political gain. The decision to make processing for the purposes of democratic engagement less transparent and to remove the balancing test that measures the impact of that processing on individual rights may indicate that the Government do not share the concern about political processing. Did the Minister's Department consider the Cambridge Analytica scandal when drawing up the provisions? Further, what safeguards will be in place to ensure that all data processing done under the new democratic engagement purpose is necessary and is not abused to spread misinformation?

Sir John Whittingdale: I would only say to the hon. Lady that I have no doubt that we will consider those aspects in great detail when we get to the specific proposals in the Bill, and I shall listen with great interest to my hon. Friend the Member for Folkestone and Hythe, who played an extremely important role in uncovering what went on with Cambridge Analytica.

Damian Collins: The principle that underpinned what happened in the Cambridge Analytica scandal was the connection of Facebook profiles to the electoral register. If I understand my right hon. Friend the Minister correctly, what he is talking about would not necessarily change that situation. This could be information that the political campaign has gained anyway from a voter profile or from information that already exists in accounts it has access to on platforms such as Facebook; it would simply be attaching that, for the purposes of targeting, to people who voted in an election. The sort of personal data that Members of Parliament hold for the purposes of completing casework would not have been processed in that way. These proposals would not change in any way the ability to safeguard people's data, and companies such as Cambridge Analytica will still seek other sources of open public data to complete their work.

Sir John Whittingdale: I think my hon. Friend is right. I have no doubt that we will go into these matters in more detail when we get to those provisions. As the hon. Member for Barnsley East knows, this measure makes a very narrow change to simply extend the existing time limit within which there is protection for elected representatives to conclude casework following a general election. As we will have opportunity in due course to look at the democratic engagement exemption, I hope she will be willing to support these narrow provisions.

Stephanie Peacock: I am grateful for the Minister's reassurance, and we are happy to support them.

10.30 am

Amendment 30 agreed to.

Schedule 1, as amended, agreed to.

Clause 6

The purpose limitation

Stephanie Peacock: I beg to move amendment 69, in clause 6, page 9, leave out lines 7 to 20.

This amendment would remove the ability of the Secretary of State to amend Annex 2, so they could not make changes through secondary legislation to the way purpose limitation operates.

The Chair: With this it will be convenient to discuss clause stand part.

Stephanie Peacock: One of the key principles in article 5 of the EU GDPR is purpose limitation. The principle aims to ensure that personal data is collected by controllers only for specified, explicit and legitimate purposes. Generally speaking, it ensures that the data is not further processed in a manner that is incompatible with those purposes. If a controller's purposes change over time, or they want to use data for a new purpose that they did not originally anticipate, they can go ahead only if the new purpose is compatible with the original purpose, they get the individual's specific consent for the new purpose or they can point to a clear legal provision requiring or allowing the new processing in the public interest.

Specifying the reasons for obtaining data from the outset helps controllers to be accountable for their processing and helps individuals understand how their data is being used and whether they are happy with that, particularly where they are deciding whether to

[Stephanie Peacock]

provide consent. Purpose limitation exists so that it is clear why personal data is being collected and what the intention behind using it is.

In any circumstance where we water down this principle, we reduce transparency, we reduce individuals' ability to understand how their data will be used and, in doing so, we weaken assurances that people's data will be used in ways that are fair and lawful. We must therefore think clearly about what is included in clause 6 and the associated annex. Indeed, many stakeholders, from Which? to Defend Digital Me, have expressed concern that what is contained in annex 2 could seriously undermine the principle of purpose limitation.

As Reset.tech illustrates, under the current regime, if data collected for a relatively everyday purpose, such as running a small business, is requested by a second controller for the purpose of investigating crime, the small business would need to assess whether this further processing—thereby making a disclosure of the data—was compatible with its original purpose. In many cases, there will be no link between the original and secondary purposes, and there are potential negative consequences for the data subjects. As such, the further processing would be unlawful, as it would breach the principle of purpose limitation.

However, under the new regime, all it would take for the disclosure to be deemed compatible with the original purpose is the second controller stating that it requires the data for processing in the public interest. In essence, this means that, for every item listed in annex 2, there are an increased number of circumstances in which data subjects' personal information could be used for purposes outside their reasonable expectations. It seems logical, therefore, that whatever is contained in the list is absolutely necessary for the public good and is subject to the highest level of public scrutiny possible.

Instead, the clause gives the Secretary of State new Henry VIII powers to add to the new list of compatible purposes by secondary legislation whenever they wish, with no provisions made for consulting on, scrutinising or assessing the impact of such changes. It is important to remember here that secondary legislation is absolutely not a substitute for parliamentary scrutiny of primary legislation. Delegated legislation, as we have discussed, is rarely voted on, and even when it is, the Government of the day will win such a vote if they have a majority.

If there are other circumstances in which the Government think it should be lawful to carry out further processing beyond the original purpose, those should be in the Bill, rather than being left to Ministers to determine at a later date, avoiding the same level of scrutiny.

The Government's impact assessment says that clarity on the reuse of data could help to fix the market failure caused by information gaps on how purpose limitation works. Providing such clarity is something we could all get behind. However, by giving the Secretary of State sweeping powers fundamentally to change how purpose limitation operates, the clause goes far beyond increasing clarity.

Improved and updated guidance on how the new rules surrounding reusing data work would be far more fruitful in providing clarity than further deregulation in this instance. If Ministers believe there are things missing from the clause and annex, they should discuss them here and now, rather than opening the back door to making further additions afterwards, and that is what the amendment seeks to ensure.

Sir John Whittingdale: The clause sets out the conditions under which the reuse of personal data for a new purpose is permitted. As the hon. Lady has said, the clause expands on the purpose limitation principle. That key principle of data protection ensures that an individual's personal data is reused only in ways they might reasonably expect.

The current provisions in the UK GDPR on personal data reuse are difficult for controllers and individuals to navigate. That has led to uncertainty about when controllers can reuse personal data. The clause addresses the existing uncertainty around reusing personal data by setting out clearly when it is permitted. That includes when personal data is being reused for a very different purpose from that for which it was originally collected—for example, when a company might wish to disclose personal data for crime prevention.

The clause permits reuse of personal data by a controller when the new purpose is "compatible"; they get fresh consent; there is a research purpose; UK GDPR is being complied with, such as for anonymisation or pseudonymisation purposes; there is an objective in the public interest authorised by law; and certain specified objectives in the public interest set out in a limited list in schedule 2 are met. I will speak more about that when we come to the amendment and the debate on schedule 2.

The clause contains a power to add or amend conditions or remove conditions added by regulations from that list to ensure it can be kept up to date with any future developments in how personal data should be reused in the public interest. It also sets out restrictions on reusing personal data that the controller originally collected on the basis of consent.

The Government want to ensure that consent is respected to uphold transparency and maintain high data protection standards. If a person gives consent for their data to be processed for a specific purpose, that purpose should be changed without their consent only in limited situations, such as for certain public interest purposes, if it would be unreasonable to seek fresh consent. That acts as a safeguard to ensure that organisations address the possibility of seeking fresh consent before relying on any exemptions.

The restrictions around consent relate to personal data collected under paragraph 1(a) of article 6 of the UK GDPR, which came into force in May 2018. Therefore, they do not apply to personal data processed on the basis of consent prior to May 2018, when different requirements applied. By simplifying the rules on further processing, the clause will give controllers legal certainty on when they can reuse personal data and give individuals greater transparency. I support the clause standing part of the Bill.

Let me turn to amendment 69, which proposes to remove the power set out in the clause to amend the annex in schedule 2. As I have already said, schedule 2 will insert a new annex in the UK GDPR, which sets out certain specific public interest circumstances where personal data reuse is permitted. The list is strictly limited and exhaustive, so a power is needed to ensure that it is kept up to date with any future developments in how personal data is reused for important public interest purposes. That builds on an existing power in

schedule 2 to the Data Protection Act 2018, where there is already the ability to make exceptions to the purpose limitation principle via secondary legislation.

The power in the clause also provides the possibility of narrowing a listed objective if there is evidence of any of the routes not being used appropriately. That includes limiting it, by reference, to the lawful ground of the original processing—for example, to prohibit the reuse of data that was collected on the basis of an individual's consent.

I would like to reassure the hon. Lady that this power will be used only when necessary and in the public interest. That is why the clause contains a restriction on its use; it may be used only to safeguard an objective listed in article 23 of the UK GDPR. Clause 44 of the Bill also requires that the Secretary of State must consult the commissioner, and any other persons as the Secretary of State considers appropriate, before making any regulations.

On that basis, I hope the hon. Lady will accept that the amendment is unnecessary.

Stephanie Peacock: The purpose behind our amendment —this speaks to a number of our amendments—is that we disagree with the amount of power being given to the Secretary of State. For that reason, I would like to continue with my amendment.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 5]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Clause 6 ordered to stand part of the Bill.

Schedule 2

PURPOSE LIMITATION: PROCESSING TO BE TREATED AS COMPATIBLE WITH ORIGINAL PURPOSE

Stephanie Peacock: I beg to move amendment 71, in schedule 2, page 138, line 16, leave out "states" and insert "confirms".

This amendment would require a person who needs personal data for a purpose described in Article 6(1)(e) (a task carried out in the public interest or in the exercise of official authority vested in the controller) to confirm, and not merely to state, that they need the data for legitimate purposes.

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

Amendment 70, in schedule 2, page 139, line 30, at end insert

"levied by a public authority".

This amendment would clarify that personal data could be processed as a "legitimate interest" under this paragraph only when the processing is carried out for the purposes of the assessment or collection of a tax or duty or an imposition of a similar nature levied by a public authority.

That schedule 2 be the Second schedule to the Bill.

Stephanie Peacock: I will begin by addressing amendment 70, which seeks only to make a wording change so that the annex cannot be misinterpreted. Paragraph 10 of annex 2 outlines that further processing is to be treated as compatible with original purposes

"where the processing is carried out for the purposes of the assessment or collection of a tax or duty or an imposition of a similar nature."

Which? has expressed concerns that that is much too vaguely worded, especially without a definition of "tax" or "duty" for the purposes of that paragraph, leaving the data open to commercial uses beyond the intention. Amendment 70 would close any potential loopholes by linking the condition to meeting a specific statutory obligation to co-operate with a public authority such as His Majesty's Revenue and Customs.

Moving on, amendment 71 would correct a similar oversight in paragraph 1 of annex 2, which was identified by the AWO and Reset.tech. Paragraph 1 aims to ensure that processing is treated as compatible with the original purpose when it is necessary for making a disclosure of personal data to another controller that needs to process that data for a task in the public interest or in the exercise of official authority and that has requested that data. However, the Bill says that processing is to be treated as compatible with the original purpose where such a request simply "states" that the other person needs the personal data for the purposes of carrying out processing that is a matter of public task. At very least, those matters should surely be actually true, rather than just stated. Amendment 71 would close that loophole, so that the request must confirm a genuine need for data in completing a task in the public interest or exercising official authority, rather than simply being a statement of need.

Beyond those amendments, I wish only to reiterate the thoughts that I expressed during the debate on clause 6. Everything contained in the annex provides for further processing that is hidden from data subjects and may not be within their reasonable expectations. The reliance on the new annex should therefore be closely monitored to ensure that it is not being exploited, or we risk compromising the purpose limitation principle altogether. Does the Department plan to monitor how the new exemptions on the reuse of data are being relied on?

10.45 am

Sir John Whittingdale: As we have already discussed with clause 6, schedule 2 inserts a new annex into the UK GDPR. It sets out certain specific public interest circumstances in which personal data reuse is permitted regardless of the purpose for which the data was originally collected—for example, when the disclosure of personal data is necessary to safeguard vulnerable individuals. Taken together, clause 6 and schedule 2 will give controllers legal certainty on when they can reuse personal data and give individuals greater transparency.

[Sir John Whittingdale]

Amendment 70 concerns taxation purposes, which are included in the list in schedule 2. I reassure the hon. Member for Barnsley East that the exemption for taxation is not new: it has been moved from schedule 2 to the Data Protection Act 2018. Indeed, the specific language in question goes back as far as 1998. We are not aware of any problems caused by that language.

The inclusion in the schedule of

"levied by a public authority"

would likely cause problems, since taxes and duties can be imposed only by law. Some must be assessed or charged by public authorities, but many become payable as a result of a person's transactions or circumstances, without any intervention needed except to enforce collection if unpaid. They are not technically levied by a public authority. That would therefore lead to uncertainty and confusion about whether processing for certain important taxation purposes would be permitted under the provision.

I hope to reassure the hon. Lady by emphasising that taxation is not included in the annex 1 list of legitimate interests. That means that anyone seeking to use the legitimate interest lawful ground for that purpose would need to carry out a balancing-of-interests test, unless they were responding to a request for information from a public authority or other body with public tasks set out in law. For those reasons, I am afraid I am unable to accept the amendment, and I hope the hon. Lady will withdraw it.

Amendment 71 relates to the first paragraph in new annex 2 to the UK GDPR, as inserted by schedule 2. The purpose of that provision is to clarify that non-public bodies can disclose personal data to other bodies in certain situations to help those bodies to deliver public interest tasks in circumstances in which personal data might have been collected for a different purpose. For example, it might be necessary for a commercial organisation to disclose personal data to a regulator on an inquiry so that that body can carry out its public functions. The provision is tightly formulated and will permit disclosure from one body to another only if the requesting organisation states that it has a public interest task, that it has an appropriate legal basis for processing the data set out in law, and that the use of the data is necessary to safeguard important public policy or other objectives listed in article 23.

I recognise that the amendment is aimed at ensuring that the requesting organisation has a genuine basis for asking for the data, but suggest that changing one verb in the clause from "state" to "confirm" will not make a significant difference. The key point is that non-public bodies will not be expected to hand over personal data on entirely spurious grounds, because of the safeguards that I described. On that basis, I hope the hon. Lady will withdraw her amendment.

Stephanie Peacock: I am reassured by what the Minister said about amendment 70 and am happy not to move it, but I am afraid he has not addressed all my concerns in respect of amendment 71, so I will press it to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 6]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Schedule 2 agreed to.

Clause 7

VEXATIOUS OR EXCESSIVE REQUESTS BY DATA SUBJECTS

Stephanie Peacock: I beg to move amendment 74, in clause 7, page 10, line 34, at end insert—

"6. Where a controller—

(a) charges a fee for dealing with a request, in accordance with paragraph 2(a), or

(b) refuses to act on a request, in accordance with paragraph 2(b)

the controller must issue a notice to the data subject explaining the reasons why they are refusing to act on the request, or charging a fee for dealing with the request, and informing the subject of their right to make a complaint to the Commissioner and of their ability to seek to enforce this right through a judicial remedy."

This amendment would oblige controllers to issue a notice to the data subject explaining the reasons why they are not complying with a request, or charging for a request, their right to make a complaint to the ICO, and their ability to seek to enforce this right through a judicial remedy.

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

Amendment 73, in clause 7, page 12, line 20, at end insert—

"(1A) When considering the resources available to the recipient for the purposes of subsection (1)(c), no account may be taken of any lack of resources which is due to a failure by the recipient to appoint staff to relevant roles where the recipient has the resources to do so."

This amendment would make it clear that, when taking into account "resources available to the controller" for deciding whether a subject access request is vexatious or excessive, this cannot include where the organisation has neglected to appoint staff, but has the finances or resources to do so.

Amendment 72, in clause 7, page 12, line 25, at end insert—

"(3) The Commissioner must prepare a code of practice under section 124A on the circumstances in which a request may be deemed vexatious or excessive.

(4) The code of practice prepared under subsection (3) must include examples of requests which may be deemed vexatious or excessive, and of requests which may be troublesome to deal with but which should not be deemed vexatious or excessive."

This amendment would require the ICO to produce a code of practice on how the terms vexatious and excessive are to be applied, with examples of the kind of requests that may be troublesome to deal with, but are neither vexatious nor excessive.

Clause stand part.

Stephanie Peacock: I will speak first to clause 7 and amendment 72. Currently, everyone has the right to ask an organisation whether or not it is using or storing their personal data and to ask for copies of that data. That is called the right of access, and exercising that right is known as making a subject access request. Stakeholders from across the spectrum, including tech companies and civil society organisations, all recognise the value of SARs in helping individuals to understand how and why their data is being used and enabling them to hold controllers to account in processing their data lawfully.

The right of access is key to transparency and often underpins people's ability to exercise their other rights as data subjects. After all, how is someone to know that their data is being used in an unlawful way, or in a way they would object to, if they are not able to ascertain whether their personal data is being held or processed by any particular organisation? For example, as the TUC highlighted in oral evidence to the Committee, the right of data subjects to make an information access request is a particularly important process for workers and their representatives, as it enables workers to gain access to personal data on them that is held by their employer and aids transparency over how algorithmic management systems operate.

It has pleased many across the board to see the Government roll back on their suggestion of introducing a nominal fee for subject access requests. However, the Bill introduces a new threshold for when controllers are able to charge a reasonable fee, or refuse a subject access request, moving from "manifestly unfounded or excessive" to "vexatious or excessive". When deciding whether a request is vexatious or excessive, the Bill requires the controller to have regard to the circumstances of the subject access request. That includes, but is not limited to, the nature of the request; the relationship between subject and controller; the resources available to the controller; the extent to which the request repeats a previous request made by the subject; how long ago any previous request was made; and whether the request overlaps with other requests made by the data subject to the controller.

Stakeholders such as the TUC, the Public Law Project and Which? have expressed concerns that, as currently drafted, the terms that make up the new threshold are too subjective and could be open to abuse by controllers who may define any request they do not want to answer as vexatious or excessive. Currently, all there is in the Bill to guide controllers on how to apply the threshold is a non-exhaustive list of considerations; as I raised on Second Reading, if that list is non-exhaustive, what explicit protections will be in place to stop the application of terms such as "vexatious" and "excessive" being stretched and manipulated by controllers who simply do not want to fulfil the requests they do not like?

There are concerns that without further guidance even the considerations listed could be interpreted selfishly by controllers who lack a desire to complete a request. For example, given that many subject access requests come from applicants who are suspicious of how their data is being used, or have cause to believe their data is being misused, there is a high likelihood that the relationship any given applicant has with the controller has previously involved some level of friction and, perhaps, anger. The Bill prompts controllers to consider their relationship with a data subject when determining whether their request is vexatious; what is to stop a controller simply marking any data subject who has shared suspicions as "angry and vexatious", thereby giving them grounds to refuse a genuine request?

Without clarity on how both the new threshold and the considerations apply, the ability of data subjects to raise a legal complaint about why their request was categorised as vexatious and excessive will be severely impeded. As AWO pointed out in oral evidence, that kind of legal dispute over a subject access request may be only the first stage of court proceedings for an individual, with a further legal case on the contents of the subject access request potentially coming afterwards. There simply should not be such a long timescale and set of legal proceedings in order for a person to exercise their fundamental data rights. Even the Information Commissioner himself, despite saying that he was clear on how the phrases "vexatious" and "excessive" should be applied, mentioned to the Committee that it was right to point out that such phrases were open to numerous interpretations.

The ICO is in a great position to provide clear statutory guidance on the application of the terms, with specific examples of when they do and do not apply, so that only truly bad-natured requests that are designed to exploit the system can be rejected or charged for. Such guidance would provide clarity on the ways in which a request might be considered troublesome but neither vexatious nor excessive. That way, controllers can be sure that they have dismissed, or charged for, only requests that genuinely pass the threshold, and data subjects can be assured that they will still be able to freely access information on how their data is being used, should they genuinely need or want it.

On amendment 73, one consideration that the Bill suggests controllers rely on when deciding whether a request is vexatious or excessive is the "resources available" to them. I assume that consideration is designed to operate in relation to the "excessive" threshold and the ability to charge. For example, when a subject access request would require work far beyond the means of the controller in question, the controller would be able to charge for providing the information needed, to ensure that they do not experience a genuine crisis of resources as a result of the request. However, the Bill does not explicitly express that, meaning the consideration in its vague form could be applied in circumstances beyond that design.

Indeed, if a controller neglected to appoint an appropriate number of staff to the responsibility of responding to subject access requests, despite having the finances and resources to do so, they could manipulate the consideration to say that any request they did not like was excessive, as a result of the limited resources available to respond. As is the case across many parts of the Bill, we cannot have legislation that simply assumes that people will act in good faith; we must instead have legislation that explicitly protects against bad-faith interpretations. The amendment would ensure just that by clarifying that a controller cannot claim that a request is excessive simply because they have neglected to arrange their resources in such a way that makes responding to the request possible.

On amendment 74, as is the case with the definition of personal data in clause 1, where the onus is placed on controllers to decide whether a living individual could

[Stephanie Peacock]

reasonably be identified in any dataset, clause 7 again places the power—this time to decide whether a request is vexatious or excessive—in the hands of the controller.

As the ICO notes, transparency around the use of data is fundamentally linked to fairness, and is about being

"clear, open and honest with people from the start about who you are, and how and why you use their personal data".

If a controller decides, then, that due to a request being vexatious or excessive they cannot provide transparency on how they are processing an individual's data at that time, the very least they could do, in the interests of upholding fairness, is to provide transparency on their justification for classifying a request in that way. The amendment would allow for just that, by requiring controllers to issue a notice to the data subject explaining the grounds on which their request has been deemed vexatious or excessive and informing them of their rights to make a complaint or seek legal redress.

In oral evidence, the Public Law Project described the Bill's lack of a requirement for controllers to notify subjects as to why their request has been rejected as a decision that creates an "information asymmetry". That is particularly concerning given that it is often exactly that kind of information that is needed to access the other rights and safeguards outlined in the Bill and across GDPR. A commitment to transparency, as the amendment would ensure, would not only give data subjects clarity on why their request had been rejected or required payment, but provide accountability for controllers who rely on the clause, and thereby a deterrent from misusing it to reject any requests that they dislike. For controllers, the workload of issuing such notices should surely be less than that of processing a request that is genuinely vexatious and excessive, ensuring that the provision does not counterbalance the benefits brought to controllers through the clause.

Sir John Whittingdale: Let me start by recognising the importance of of subject access requests. I am aware that some have interpreted the change in the wording for grounds of refusal as a weakening. We do not believe that is the case.

On amendment 72, in our view the new "vexatious or excessive" language in the Bill gives greater clarity than there has previously been. The Government have set out parameters and examples in the Bill that outline how the term "vexatious" should be interpreted within a personal data protection context, to ensure that controllers understand.

11 am

The power to request codes of practice exists in the legislation and should be relied on to request any new codes. That power provides a route for the Secretary of State to require the Information Commissioner to prepare any code of practice that gives guidance on good practice in the processing of personal data. However, there will be situations where non-statutory guidance, which can be produced without being requested under regulations made by the Secretary of State, may be more appropriate than a statutory code of practice.

Examples of when a request may or may not be vexatious or excessive are best placed in non-statutory guidance produced by the ICO, as that will provide the flexibility to amend and change those examples whenever necessary. A wider code of practice on subject access requests may be a useful tool to create clarity. However, the Government want to work with the ICO to set out the scope of any code, in consultation with affected stakeholders, before using the power to request it.

Amendment 73 focuses on the new parameters for controllers to consider when determining whether a request is vexatious or excessive. The parameters include

"resources available to the controller",

thereby emphasising the importance of proportionality when considering whether a request is vexatious or excessive.

Damian Collins: Does my right hon. Friend agree that the provisions will be helpful and important for organisations that gather data about public persons, and particularly oligarchs, who are very adept at using subject access requests to bombard and overwhelm a journalist or a small investigatory team that is doing important work looking into their business activities?

Sir John Whittingdale: I completely agree with my hon. Friend. That is an issue that both he and I regard as very serious, and is perhaps another example of the kind of legal tactic that SLAPPs—strategic lawsuits against public participation—represent, whereby oligarchs can frustrate genuine journalism or investigation. He is absolutely right to emphasise that.

It is important to highlight that controllers can already consider resource when refusing or charging a reasonable fee for a request. The Government do not wish to change that situation. Current ICO guidance sets out that controllers can consider resources as a factor when determining if a request is excessive.

The new parameters are not intended to be reasons for refusal. The Government expect that the new parameters will be considered individually as well as in relation to one another, and a controller should consider which parameters may be relevant when deciding how to respond to a request. For example, when the resource impact of responding would be minimal even if a large amount of information was requested—such as for a large organisation—that should be taken into account. Additionally, the current rights of appeal allow a data subject to contest a refusal and ultimately raise a complaint with the ICO. Those rights will not change with regard to individual rights requests.

Amendment 74 proposes adding more detail on the obligations of a controller who refuses or charges for a request from a data subject. The current legislation sets out that any request from a data subject, including subject access requests, is to be responded to. The Government are retaining that approach and controllers will be expected to demonstrate why the provision applies each time it is relied on. The current ICO guidance sets out those obligations on controllers and the Government do not plan to suggest a move away from that approach.

The clause also states that it is for the controller to show that a request is vexatious or excessive in circumstances where that might be in doubt. Thus, the Government believe that the existing legislation provides the necessary protections. Following the passage of the

Bill, the Government will work with the ICO to update guidance on subject access requests, which we believe plays an important role and is the best way to achieve the intended effect of the amendments. For those reasons, I will not accept this group of amendments; I hope that the hon. Member for Barnsley East will be willing to withdraw them.

I turn to clause 7 itself. As I said, the UK's data protection framework sets out key data subject rights, including the right of access—the right for a person to obtain a copy of their personal data. A subject access request is used when an individual requests their personal data from an organisation. The Government absolutely recognise the importance of the right of access and do not want to restrict that right for reasonable requests.

The existing legislation enables organisations to refuse or charge a reasonable fee for a request when they deem it to be "manifestly unfounded or excessive". Some organisations, however, struggle to rely on that in cases where it may be appropriate to do so, which as a consequence impacts their ability to respond to reasonable requests.

The clause changes the legislation to allow controllers to refuse or charge a reasonable fee for a request that is "vexatious or excessive". The clause adds parameters for controllers to consider when relying on the "vexatious or excessive" exemption, such as the nature of the request and the relationship between the data subject and the controller. The clause also includes examples of the types of request that may be vexatious, such as those intended to cause distress, those not made in good faith or those that are an abuse of process.

We believe that the changes will give organisations much-needed clarity over when they can refuse or charge a reasonable fee for a request. That will ensure that controllers can focus on responding to reasonable requests, as well as other important data and organisational needs. I commend the clause to the Committee.

Stephanie Peacock: I appreciate that, as the Minister said, the Government do not intend the new terms to be grounds for refusal, but his remarks do not reassure me that that will not be the case. Furthermore, as I said on moving the amendment, stakeholders such as the TUC, Public Law and Which? have all expressed concern that, as drafted, those terms are too subjective. I will press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 7]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Amendment proposed: 73, in clause 7, page 12, line 20, at end insert—

"(1A) When considering the resources available to the recipient for the purposes of subsection (1)(c), no account may be taken of any lack of resources which is due to a failure by the recipient to appoint staff to relevant roles where the recipient has the resources to do so."—*(Stephanie Peacock.)*

This amendment would make it clear that, when taking into account "resources available to the controller" for deciding whether a subject access request is vexatious or excessive, this cannot include where the organisation has neglected to appoint staff, but has the finances or resources to do so.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 8]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Amendment proposed: 72, in clause 7, page 12, line 25, at end insert—

"(3) The Commissioner must prepare a code of practice under section 124A on the circumstances in which a request may be deemed vexatious or excessive.

(4) The code of practice prepared under subsection (3) must include examples of requests which may be deemed vexatious or excessive, and of requests which may be troublesome to deal with but which should not be deemed vexatious or excessive."—*(Stephanie Peacock.)*

This amendment would require the ICO to produce a code of practice on how the terms vexatious and excessive are to be applied, with examples of the kind of requests that may be troublesome to deal with, but are neither vexatious nor excessive.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 9]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

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

The Committee divided: Ayes 9, Noes 6.

Division No. 10]

AYES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

NOES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

Question accordingly agreed to.

Clause 7 ordered to stand part of the Bill.

Clause 8

TIME LIMITS FOR RESPONDING TO REQUESTS BY DATA SUBJECTS

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

Sir John Whittingdale: Clause 8 makes changes to the time requirements to which an organisation must adhere when responding to a subject access request. Currently, organisations must respond to a subject access request within a set period; in the majority of cases, that is one month from receipt of the request. This clause enables organisations to "stop the clock" on the response time when an organisation is unable to respond without further information or clarification from an individual. For example, when the controller has information on multiple data subjects with the same name, they may require further information to help to differentiate the data subject's information from others'. Organisations must have a legitimate reason to pause the response time; once confirmation is received from the data subject, the original time obligations resume.

The clause will also enable organisations to extend the period permitted for law enforcement and the intelligence services to respond to complex requests by two further months in certain circumstances. This replicates the existing provisions applicable to processing requests under the UK GDPR. Currently, all subject access requests received under the law enforcement and intelligence services regimes must be actioned within one month, irrespective of the complexity or number of requests received from an individual. Consequently, complex or confusing requests can disproportionately burden public bodies operating under those regimes, creating resource pressures.

Clause 8 will rectify the disparity currently existing between processing regimes and put law enforcement and intelligence services organisations on an equal footing to UK GDPR organisations. That will also provide a consistent framework for organisations operating under more than one regime at the same time. The clause also brings clarity on how best to respond to a confusing or complex request, ensuring that organisations do not lose time while seeking this clarification and can instead focus on responding to a request. On that basis, I urge that clause 8 stand part of the Bill.

11.15 am

Stephanie Peacock: I expressed my thoughts on the value and importance of subject access requests when we debated clause 7, and most of the same views remain pertinent here. Clause 8 allows for subject access requests to be extended where the nature of the request is complex, or due to volume. Some civil society groups, including Reset.tech, have expressed concern that that could mean that requests are unduly delayed for months, reflecting concern that they could be disregarded altogether, which was discussed when we debated clause 7. With that in mind, can the Minister tell us what protections will be in place to ensure that data controllers do not abuse the new ability to extend subject access requests, particularly by using the excuse that it is a large amount of data, in order to delay requests that they simply do not wish to respond to?

The clause provides some clarity on clause 7 by demonstrating that just because a request is lengthy or comes in combination with many others, it is not necessarily excessive as the clause gives controllers the option to extend the timeframe for dealing with requests that are high in volume. Of course, we do not want to unnecessarily delay requests, but allowing controllers to manage their load within a reasonable extended timeframe can act as a safeguard against their automatically relying on the "excessive" threshold. With that in mind, I am happy for the clause to stand part. However, I reiterate that my comments on clause 7 should be referred to.

Sir John Whittingdale: May I briefly respond to the hon. Lady's comments? I assure her that controllers will not be able to stop the clock for all subject access requests—only for those where they reasonably require further information to be able to proceed with responding. Once that information has been received from a data subject, the clock resumes and the controller must proceed with responding to the request within the applicable time period, which is usually one month from when the controller receives the request information. A data subject who has provided the requested information would also be able to complain to a controller, and ultimately to the Information Commissioner's Office, if they feel that their request has not been processed within the appropriate time. I hope the hon. Lady will be assured that there are safeguards to ensure that this power is not abused.

Question put and agreed to.

Clause 8 accordingly ordered to stand part of the Bill.

Clause 9

INFORMATION TO BE PROVIDED TO DATA SUBJECTS

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

The Chair: With this it will be convenient to discuss clause 10 stand part.

Sir John Whittingdale: Clause 9 provides researchers, archivists and those processing personal data for statistical purposes with a new exemption from providing certain information to individuals when they are reusing datasets for a different purpose, which will help to ensure that important research can continue unimpeded. The new exemption will apply when the data was collected directly from the individual, and can be used only when providing the additional information would involve a disproportionate

effort. There is already an exemption from this requirement where the personal data was collected from a different source.

The clause also adds a non-exhaustive list of examples of factors that may constitute a disproportionate effort. This list is added to both the new exemption in article 13 and the existing exemption found in article 14. Articles 13 and 14 of the UK GDPR set out the information that must be provided to data subjects at the point of data collection: article 13 covers circumstances where data is directly collected from data subjects, and article 14 covers circumstances where personal data is collected indirectly—for example, via another organisation. The information that controllers must provide to individuals includes details such as the identity and contact details of the controller, the purposes of the processing and the lawful basis for processing the data.

Given the long-term nature of research, it is not always possible to meaningfully recontact individuals. Therefore, applying a disproportionate effort exemption addresses the specific problem of researchers wishing to reuse data collected directly from an individual. The exemption will help ensure that important research can continue unimpeded. The clause also makes some minor changes to article 14. Those do not amend the scope of the exemption or affect its operation, but make it easier to understand.

I now turn to clause 10, which introduces an exemption relating to legally professionally privileged data into the law enforcement regime, mirroring the existing exemptions under the UK GDPR and the intelligence services regime. As a fundamental principle of our legal system, legal professional privilege protects confidential communications between professional legal advisers and their clients. The existing exemption in the UK GDPR restricts an individual's right to access personal data that is being processed or held by an organisation, and to receive certain information about that processing.

However, in the absence of an explicit exemption, organisations processing data under the law enforcement regime, for a law enforcement purpose rather than under the UK GDPR, must rely on ad hoc restrictions in the Data Protection Act. Those require them to evaluate and justify its use on a case-by-case basis, even where legal professional privilege is clearly applicable. The new exemption will make it simpler for organisations that process data for a law enforcement purpose to exempt legally privileged information, avoiding the need to justify the use of alternative exemptions. It will also clarify when such information can be withheld from the individual.

Hon. Members might wonder why an exemption for legal professional privilege was not included under the law enforcement regime of the Data Protection Act in the first place. The reason is that we faithfully transposed the EU law enforcement directive, which did not contain such an exemption. Following our exit from the EU, we are taking this opportunity to align better the UK GDPR and the law enforcement regime, thereby simplifying the obligations for organisations and clarifying the rules for individuals.

Stephanie Peacock: The impact of clause 9 and the concerns around it should primarily be understood in relation to the definition contained in clause 2, so I refer hon. Members to my remarks in the debate on clause 2. I also refer them to my remarks on purpose limitation in clause 6. To reiterate both in combination, I should say that purpose limitation exists so that it is clear why personal data is being collected, and what the intention is behind its use. That means that people's data should not largely be reused in ways not initially collected for, unless a new legal basis is obtained.

It is understandable that, where genuine scientific, historical and statistical research is occurring, and there is disproportionate effort to provide the information required to data subjects, there may be a need for exemption and to reuse data without informing the subject. However, that must be done only where strictly necessary. We must be clear that, unless there are proper boundaries to the definition of scientific data, this could be interpreted far too loosely.

I am concerned that, without amendment to clause 2, clause 9 could extend the problem of scientific research being used as a guise for using people's personal data in malicious or pseudoscientific ways. Will the Minister tell us what protections will be in place to ensure that people's data is not reused on scientific grounds for something that they would otherwise have objected to?

On clause 10, I will speak more broadly on law enforcement processing later in the Bill, but it is good to have clarity on the legal professional privilege exemptions. I have no further comments at this stage.

Carol Monaghan (Glasgow North West) (SNP): What we are basically doing is changing the rights of individuals, who would previously have known when their data was used for a purpose other than that for which it was collected. The terms

"scientific or historical research, the purposes of archiving in the public interest or statistical purposes"

are very vague, and, according to the Public Law Project, open to wide interpretation. Scientific research is defined as "any research that can reasonably described as scientific, whether publicly or privately funded".

I ask the Minister: what protections are in place to ensure that private companies are not given, through this clause, a carte blanche to use personal data for the purpose of developing new products, without the need to inform the data subject?

Sir John Whittingdale: These clauses relate to one of the fundamental purposes of the Bill, which is to facilitate genuine scientific research—obviously, that carries with it huge potential benefits in the areas of tackling disease or other scientific advances. We debated the definition of scientific research earlier in relation to clause 2. We believe that the definition is clear. In this particular case, the use of historical data can be very valuable. It is simply impractical for some organisations to reobtain consent when they may not even know where original data subjects are now located.

The Chair: Order. I apologise to the Minister. He can resume his remarks at 2 o'clock, when we meet again in this room but, it being 11.25 am, the Committee is now adjourned.

11.25 am

The Chair adjourned the Committee without Question put (Standing Order No. 88).

Adjourned till this day at Two o'clock.

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Fourth Sitting

Tuesday 16 May 2023

(Afternoon)

CONTENTS

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 20 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

† Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
† Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Eastwood, Mark *(Dewsbury)* (Con)
† Henry, Darren *(Broxtowe)* (Con)
† Hunt, Jane *(Loughborough)* (Con)
† Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Monaghan, Carol *(Glasgow North West)* (SNP)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
† Richards, Nicola *(West Bromwich East)* (Con)
† Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 16 May 2023

(Afternoon)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

Clause 9

Information to be provided to data subjects

2 pm

Question (this day) again proposed, That the clause stand part of the Bill.

The Chair: I remind the Committee that with this we are discussing clause 10 stand part.

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): When the Committee adjourned this morning, I was nearly at my conclusion; I was responding to points made by the hon. Member for Barnsley East and by the hon. Member for Glasgow North West, who has not yet rejoined us. I was saying that the exemption applies where the data originally collected is historic, where to re-contact to obtain consent would require a disproportionate effort, and where that data could be of real value in scientific research.[1] We think that there is a benefit to research and we are satisfied that the protection is there. There was some debate about the definition of scientific research, which we covered earlier; that is a point that is appealable to the Information Commissioner's Office. On the basis of what I said earlier, and that assurance, I hope that the Committee will agree to the clause.

Question put and agreed to.

Clause 9 accordingly ordered to stand part of the Bill.

Clause 10 ordered to stand part of the Bill.

Clause 11

Automated decision-making

Stephanie Peacock (Barnsley East) (Lab): I beg to move amendment 78, in clause 11, page 18, line 13, after "subject" insert "or decision subject".

This amendment, together with Amendments 79 to 101, would apply the rights given to data subjects by this clause to decision subjects (see NC12).

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

Amendment 79, in clause 11, page 18, line 15, leave out "data".

See explanatory statement to Amendment 78.

Amendment 80, in clause 11, page 18, line 16, leave out "data".

See explanatory statement to Amendment 78.

Amendment 81, in clause 11, page 18, line 27, after "subject" insert "or decision subject".

See explanatory statement to Amendment 78.

Amendment 82, in clause 11, page 18, line 31, after "subject" insert "or decision subject".

See explanatory statement to Amendment 78.

Amendment 83, in clause 11, page 19, line 4, after "subject" insert "or decision subject".

See explanatory statement to Amendment 78.

Amendment 84, in clause 11, page 19, line 7, leave out "data".

See explanatory statement to Amendment 78.

Amendment 85, in clause 11, page 19, line 11, leave out "data".

See explanatory statement to Amendment 78.

Amendment 86, in clause 11, page 19, line 12, leave out "data".

See explanatory statement to Amendment 78.

Amendment 87, in clause 11, page 19, line 13, leave out "data".

See explanatory statement to Amendment 78.

Amendment 88, in clause 11, page 19, line 15, leave out "data".

See explanatory statement to Amendment 78.

Amendment 89, in clause 11, page 19, line 17, leave out "data".

See explanatory statement to Amendment 78.

Amendment 90, in clause 11, page 19, line 26, after "subject" insert "or decision subject".

See explanatory statement to Amendment 78.

Amendment 91, in clause 11, page 20, line 8, after "subject" insert "or decision subject".

See explanatory statement to Amendment 78.

Amendment 92, in clause 11, page 20, line 10, leave out "data".

See explanatory statement to Amendment 78.

Amendment 93, in clause 11, page 20, line 12, leave out "data".

See explanatory statement to Amendment 78.

Amendment 94, in clause 11, page 20, line 23, after "subject" insert "or decision subject".

See explanatory statement to Amendment 78.

Amendment 95, in clause 11, page 20, line 28, after "subject" insert "or decision subject".

See explanatory statement to Amendment 78.

Amendment 96, in clause 11, page 20, line 31, leave out "data".

See explanatory statement to Amendment 78.

Amendment 97, in clause 11, page 20, line 35, leave out "data".

See explanatory statement to Amendment 78.

Amendment 98, in clause 11, page 20, line 37, leave out "data".

See explanatory statement to Amendment 78.

Amendment 99, in clause 11, page 20, line 39, leave out "data".

See explanatory statement to Amendment 78.

1. *[Official Report, 23 May 2023, Vol. 733, c. 1MC.]*

Amendment 100, in clause 11, page 21, line 1, leave out "data".

See explanatory statement to Amendment 78.

Amendment 101, in clause 11, page 21, line 31, after "subject" insert "or decision subject".

See explanatory statement to Amendment 78.

Amendment 106, in clause 27, page 47, line 27, after "subjects", insert "decision subjects,".

This amendment would require the ICO to have regard to decision subjects (see NC12) as well as data subjects as part of its obligations.

Amendment 108, in clause 29, page 53, line 11, at end insert—

"(ba) decision subjects;".

This amendment, together with Amendments 109 and 110, would require codes of conduct produced by the ICO to have regard to decision subjects (see NC12) as well as data subjects.

Amendment 109, in clause 29, page 53, line 13, at end insert—

"(d) persons who appear to the Commissioner to represent the interests of decision subjects.".

See explanatory statement to Amendment 108.

Amendment 110, in clause 29, page 53, line 21, after "subjects", insert ", decision subjects".

See explanatory statement to Amendment 108.

New clause 12—*Decision subjects*—

"(1) The UK GDPR is amended as follows.

(2) In Article 4, after paragraph (A1), insert—

'(A1A) "decision subject" means an identifiable individual who is subject to data-based and automated decision making;'".

This new clause would provide a definition of "decision subjects", enabling them to be given rights similar to those given to data subjects (see, for example, Amendment 78).

Stephanie Peacock: I am pleased to speak to new clause 12, which would insert a definition of decision subjects, and to amendments 79 to 101, 106 and 108 to 110, which seek to insert rights and considerations for decision subjects that mirror those of data subjects at various points throughout the Bill.

Most of our data protection legislation operates under the assumption that the only people affected by data-based and automated decision making are data subjects. The vast majority of protections available for citizens are therefore tied to being a data subject: an identifiable living person whose data has been used or processed. However, as Dr Jeni Tennison described repeatedly in evidence to the Committee, that assumption is unfortunately flawed. Although data subjects form the majority of those affected by data-based decision making, they are not the only group of people impacted. It is becoming increasingly common across healthcare, employment, education and digital platforms for algorithms created and trained on one set of people to be used to reach conclusions about another, wider set of people. That means that an algorithm can make an automated decision that affects an individual to a legal or similarly significant degree without having used their personal data specifically.

For example, as Connected by Data points out, an automated decision could be made about a neighbourhood area, such as a decision on gritting or a police patrol route, based on personal data about some of the people who live in that neighbourhood, with the outcome impacting even those residents and visitors whose data was not directly used. For those who are affected by the automated decision but are not data subjects, there is currently no protection, recognition or method of redress.

The new clause would therefore define the decision subjects who are impacted by the likes of AI without their data having been used, in the hope that we can give them protections throughout the Bill that are equal to those for data subjects, where appropriate. That is especially important because special category data is subject to stricter safeguards for data subjects but not for decision subjects.

Connected by Data illustrates that point using the following example. Imagine a profiling company that uses special category data about the mental health of some volunteers to construct a model that predicts mental health conditions based on social media feeds, which would not be special category data. From that information, the company could give an estimate of how much time people are likely to take off work. A recruitment agency could then use that model to assess candidates and reject those who are likely to have extended absences. The model would never use any special category data about the candidates directly, but those candidates would have been subject to an automated decision that made assumptions about their own special category data, based on their social media feeds. In that scenario, by virtue of being a decision subject, the individual would not have the right to the same safeguards as those who were data subjects.

Furthermore, there might be scenarios in which someone was subject to an automated decision despite having consciously prevented their personal data from being shared. Connected by Data illustrates that point by suggesting that we consider a person who has set their preferences on their web browser so that it does not retain tracking cookies or share information such as their location when they visit an online service. If the online service has collected data about the purchasing patterns of similarly anonymous users and knows that such a customer is willing to pay more for the service, it may automatically provide a personalised price on that basis. Again, no personal data about the purchaser will have been used in determining the price that they are offered, but they will still be subject to an automated decision based on the data of other people like them.

What those scenarios illustrate is that it is whether an automated decision affects an individual in a legal or similarly significant way that should be central to their rights, rather than whether any personal data is held about them. If the Bill wants to unlock innovation around AI, automated decisions and the creative use of data, it is only fair that that be balanced by ensuring that all those affected by such uses are properly protected should they need to seek redress.

This group of amendments would help our legislative framework to address the impact of AI, rather than just its inputs. The various amendments to clause 11 would extend to decision subjects rights that mirror those given to data subjects regarding automated decision making, such as the right to be informed, the right to safeguards such as contesting a decision and the right to seek human intervention. Likewise, the amendments to clauses 27 and 29 would ensure that the ICO is obliged to have regard to decision subjects both generally and when producing codes of conduct.

[Stephanie Peacock]

Finally, to enact the safeguards to which decision subjects would hopefully be entitled via the amendments to clause 11, the amendment to clause 39 would allow decision subjects to make complaints to data controllers, mirroring the rights available to data subjects. Without defining decision subjects in law, that would not be possible, and members of the general public could be left without the rights that they deserve.

Sir John Whittingdale: I am very much aware of the concern about automated decision making. The Government share the wish of the hon. Member for Barnsley East for all those who may be affected to be given protection. Where I think we differ is that we do not recognise the distinction that she tries to make between data subjects and decision subjects, which forms the basis of her amendments.

The hon. Lady's amendments would introduce to the UK GDPR a definition of the term "decision subject", which would refer to an identifiable individual subject to data-based and automated decision making, to be distinguished from the existing term "data subject". The intended effect is to extend the requirements associated with provisions related to decisions taken about an individual using personal data to those about whom decisions are taken, even though personal information about them is not held or used to take a decision. It would hence apply to the safeguards available to individuals where significant decisions are taken about them solely through automated means, as amendments 78 to 101 call for, and to the duties of the Information Commissioner to have due regard to decision subjects in addition to data subjects, as part of the obligations imposed under amendment 106.

I suggest to the hon. Lady, however, that the existing reference to data subjects already covers decision subjects, which are, if you like, a sub-group of data subjects. That is because even if an individual's personal data is not used to inform the decision taken about them, the fact that they are identifiable through the personal data that is held makes them data subjects. The term "data subject" is broad and already captures the decision subjects described in the hon. Lady's amendment, as the identification of a decision subject would make them a data subject.

I will not, at this point, go on to set out the Government's wider approach to the use of artificial intelligence, because that is somewhat outside the scope of the Bill and has already been set out in the White Paper, which is currently under consultation. Nevertheless, it is within that framework that we need to address all these issues.

Damian Collins (Folkestone and Hythe) (Con): I have been closely following the speeches of the Minister and the hon. Member for Barnsley East. The closest example that I can think of for this scenario is the use of advertising tools such as lookalike audiences on Facebook and customer match on YouTube, where a company holding data about users looks to identify other customers who are the closest possible match. It does not hold any personal data about those people, but the platform forms the intermediary to connect them. Is the Minister saying that in that situation, as far as the Bill is concerned, someone contacted through a lookalike audience has the same rights as someone who is contacted directly by an advertiser that holds their data?

Sir John Whittingdale: Essentially, if anybody is affected by automated decision making on the basis of the characteristics of another person whose data is held—in other words, if the same data is used to take a decision that affects them, even if it does not personally apply to them—they are indeed within the broader definition of a data subject. With that reassurance, I hope that the hon. Member for Barnsley East will consider withdrawing her amendment.

Stephanie Peacock: I appreciate the Minister's comments, but the point is that the data could be used—I gave the example that it might affect a group of residents who were not identifiable but were still subject to that data—so I am not quite sure that I agree with the Minister's comparison. As the use of automated decision making evolves and expands, it is crucial that even if a person's data is not being used directly, they are afforded protections and rights if they are subject to the outcome. I would like to press my amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 10.

Division No. 11]

AYES

Amesbury, Mike	Onwurah, Chi
Huq, Dr Rupa	Peacock, Stephanie
Long Bailey, Rebecca	
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

Question accordingly negatived.

Stephanie Peacock: I beg to move amendment 77, in clause 11, page 19, line 12, at end insert

"and about the safeguards available to the subject in accordance with this paragraph and any regulations under Article 22D(4);".

This amendment would require controllers proactively to provide data subjects with information about their rights in relation to automated decision-making.

The Chair: With this it will be convenient to discuss amendment 120, in clause 11, page 19, line 12, at end insert—

"(aa) require the controller to inform the data subject when a decision described in paragraph 1 has been taken in relation to the data subject;".

This amendment would require a data controller to inform a data subject whenever a significant decision about that subject based entirely or partly on personal data was taken based solely on automated processing.

Stephanie Peacock: New article 22C of the UK GDPR, inserted by clause 11, sets out the safeguards available to those who are subject to automated decision making. One such safeguard is that controllers must provide information to subjects relating to significant decisions taken through solely automated processing. That includes

notifying subjects when a decision has been taken or informing them of the logic involved in producing that decision.

That provision is important. After all, how can the subject of an automated decision possibly exercise their other rights surrounding that decision if they do not even know that it has been taken on a solely automated basis? By the same logic, however, the average member of the general public is not likely to be aware of those other rights in the first place, including the rights to express their point of view with respect to automated decisions, to contest them and to seek human intervention.

Amendment 77 therefore recommends that as well as controllers being required to inform subjects about the decision, the same notice should be used as a vehicle to ensure that the subject is aware of the rights and safeguards in place to protect them and offer them redress. It would require no extra administrative effort on behalf of the controllers, because they will already be informing subjects. A proactive offer of redress may also encourage controllers to have extra regard to the way in which their automated systems are operating, in order to avoid unlawful activity that may cause them to receive a complaint or a request for human intervention.

An imbalance of power between those who conduct automated decisions and those who are subject to them already largely exists. Those who conduct decisions hold the collective power of the data, whereas each individual subject to a decision has only their own personal information; I will address that issue in greater detail in relation to other amendments, but there is no reason why that power imbalance should be exacerbated by hiding an individual's own rights from them. If the intention of new article 22C is, as stated, to ensure that controllers are required to review and correct decisions that have produced a systematically wrongful outcome, there should be no issue with ensuring that the mechanism is properly communicated to the people it purports to serve. I am pleased to see that the hon. Member for Glasgow North West has tabled a similar amendment.

2.15 pm

Carol Monaghan (Glasgow North West) (SNP): I rise to speak to my amendment 120. The explanatory notes to the Bill clarify that newly permitted automated decisions will not require the existing legal safeguard of notification, stating only:

"Where appropriate, this may include notifying data subjects after such a decision has been taken".

Clause 11 would replace article 22 of the GDPR, which regulates AI decision making, with new articles 22A to 22D. According to Connected by Data, it is built on the faulty assumption that the people who are affected by automated decision making are data subjects—identifiable individuals within the data used to make the automated decision. However, now that AI decisions can be based on information about other people, it is becoming increasingly common for algorithms created through training on one set of people to be used to reach conclusions about another set.

A decision can be based on seemingly innocuous information such as someone's postcode or whether they liked a particular tweet. Where such a decision has an impact on viewing recommendations for an online player, we would probably not be that concerned, but personal data is being used more and more to make decisions that affect whole groups of people rather than identified individuals. We need no reminding of the controversy that ensued when Ofqual used past exam results to grade students during the pandemic.

Another example might be an electricity company getting data from its customers about home energy consumption. Based on that data, it could automatically adjust the time of day at which it offered cheaper tariffs. Everyone who used the electricity company would be affected, whether data about their energy consumption patterns were used to make the decision or not. It is whether an automated decision has a legal or similarly significant effect on an individual that should be relevant to their rights around automated decision making.

Many of the rights and interests of decision subjects are protected through the Equality Act 2010, as the Committee heard in oral evidence last week. What is not covered by other legislation, however, is how data can be used in automated decisions and the rights of decision subjects to be informed about, control and seek redress around automated decisions with a significant effect on them. According to Big Brother Watch:

"This is an unacceptable dilution of a critical safeguard that will not only create uncertainty for organisations seeking to comply, but could lead to vastly expanded ADM operating with unprecedented opacity."

Amendment 120 would require a data controller to inform a data subject whenever a significant decision about that subject was based solely on automated processing. I am pleased that the hon. Member for Barnsley East has tabled a similar amendment, which I support.

Sir John Whittingdale: The Government absolutely share hon. Members' view of the importance of transparency. We agree that individuals who are subject to automated decision making should be made aware of it and should have information about the available safeguards. However, we feel that those requirements are already built into the Bill via article 22C, which will ensure that individuals are provided with information as soon as is practicable after such decisions have been taken. This will need to include relevant information that an individual would require to contest such decisions and seek human review of them.

The reforms that we propose take an outcome-focused approach to ensure that data subjects receive the right information at the right time. The Information Commissioner's Office will play an important role in elaborating guidance on what that will entail in different circumstances.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): If I understood the Minister correctly, he said that decision subjects are a subset of data subjects. Can he envisage any circumstances in which a decision subject is not included within the group "data subjects"?

Sir John Whittingdale: It is certainly our view that anybody who is affected by an automated decision made on the basis of data held about individuals themselves becomes a data subject, so I think the answer to the honourable Lady's question is no. As I said, the Information Commissioner's Office will provide guidance in this

[Sir John Whittingdale]

area. If such a situation does arise, obviously it will need to be considered.The hon. Members for Barnsley East and for Glasgow North West asked about making information available to all those affected, and about safeguards, which we think are contained within the requirements under article 22C.

Damian Collins: Further to the point that was made earlier, let us say that a Facebook user was targeted with an advert that was based on their protected characteristics data—data relevant to their sexual orientation, for example—but that user said that they had never shared that information with the platform. Would they have the right to make a complaint, either to the advertiser or to the platform, for inferring that data about them and making it available to a commercial organisation without their informed consent?

Sir John Whittingdale: They would obviously have that right, and indeed they would ultimately have the right to appeal to the Information Commissioner if they felt that they had been subjected unfairly to a decision where they had not been properly informed of the fact. On the basis of what I have said, I hope the hon. Member for Barnsley East might withdraw her amendment.

Stephanie Peacock: I appreciate the Minister's comment, but the Government protection does not go as far as we would like. Our amendment speaks to the potential imbalance of power in the use of data and it would not require any extra administrative effort on behalf of controllers. For that reason, I will press it to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 10.

Division No. 12]

AYES

Amesbury, Mike	Onwurah, Chi
Huq, Dr Rupa	Peacock, Stephanie
Long Bailey, Rebecca	
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

Question accordingly negatived.

The Chair: Ms Monaghan, do you wish to move amendment 120 formally?

Carol Monaghan: I will not move it formally, Mr Hollobone, but I may bring it back on Report.

Stephanie Peacock: I beg to move amendment 76, in clause 11, page 19, line 34, at end insert—

"5A. The Secretary of State may not make regulations under paragraph 5 unless—

(a) following consultation with such persons as the Secretary of State considers appropriate, the Secretary of State has published an assessment of the impact of the change to be made by the regulations on the rights and freedoms of data and decision subjects (with particular reference to children),

(b) the Commissioner has reviewed the Secretary of State's statement and published a statement of the Commissioner's views on whether the change should be made, with reasons, and

(c) the Secretary of State has considered whether to proceed with the change in the light of the Commissioner's statement."

This amendment would make the Secretary of State's ability to amend the safeguards for automated decision-making set out in new Articles 22A to D subject to a requirement for consultation with interested parties and with the Information Commissioner, who would be required to publish their views on any proposed change.

The Chair: With this it will be convenient to discuss amendment 75, in clause 11, page 19, line 36, at end insert—

"7. The Commissioner must prepare a code of practice under section 124A of the Data Protection Act 2018 on the interpretation of references in this Regulation to "meaningful human involvement" and "similarly significant".

8. The code of practice prepared under paragraph 7 must include examples of the kinds of processing which do, and which do not, fall within the definitions which use the terms referred to in that paragraph."

This amendment would require the ICO to produce a code of practice on the interpretation of references to "meaningful human involvement" and "similarly significant" in connection with automated decision-making, with examples of the kinds of processing that would not count as falling within these definitions.

Stephanie Peacock: I will begin by discussing amendment 76 in the context of the general principles of this clause. The rise of AI and algorithmic decision making has happened at an unprecedented speed—so much so, in fact, that when the first version of this Bill was published, the likes of ChatGPT were not even launched yet. Now we live in a world where the majority of people across the country have been affected by or have used some form of AI-based or automated decision-making system.

When algorithms and automation work well, not only do they reduce administrative burdens, increase efficiency and free up capacity for further innovation and growth; they can also have remarkable outcomes. Indeed, PwC UK suggests that UK GDP could be up to 10.3% higher in 2030 as a result of artificial intelligence. AI is already being used to develop vaccines and medicines, for example, which are saving lives across the country and the entire world. Labour's belief, outlined in our industrial strategy, is that the UK should be leading the world on efforts to ensure that transformative AI is aligned with the public interest in that way, and that regulations ensure we are well positioned to do that.

Despite the potential of AI to be harnessed for the public good, however, where things go wrong, the harms can be serious. The first way in which automation is prone to go wrong is by producing discriminatory outcomes. An algorithm, although intelligent in itself, is only ever as fair as the information and the people used to train it. That means that where biases exist in our world, they can become entrenched in our automated systems too.

In in 2020, thousands of students in England and Wales received A-level exam results where, due to the pandemic, their grades were determined by an algorithm rather than by sitting an exam. At the hands of the automated system, almost 40% of students received grades lower than they had anticipated, with pupils from certain backgrounds and areas such as those that I represent disproportionately impacted by the lower marks. Within days of the results being published, there was widespread public outcry about the distress caused, as well as threats of mass protests and legal action. Similarly, Amazon was reported to have used an AI tool that systematically penalised women in job application processes. The tool had been trained on a decade's worth of CVs, predominantly submitted by men. As such examples show, AI on its own can produce discriminatory outcomes. Our regulation must therefore recognise that and seek to protect against it.

The second major way in which automated decision making tends to go wrong, or can be abused, is when it makes legal or critical decisions about our lives based on mismanaged, abused or faulty systems. In the most extreme cases, automated systems can even contribute to deciding whether someone's employment will be terminated, with grave consequences when that goes wrong. As mentioned in the oral evidence sessions, for example, last month the courts upheld the finding that three UK-based Uber drivers were robotically fired without redress, having been accused of fraudulent activity on the basis of an automated detection system. The court found that human involvement in the firing process was

"not much more than a purely symbolic act",

and that implementing such a decision without a mechanism for appeal was unjust. Where livelihoods are at risk, data regulation must ensure that proper safeguards are in place to protect against mismanaged and faulty automated systems.

Serious harms sometimes occur under the existing system, but there are laws under the GDPR that try to protect us against discriminatory outcomes and mismanagement. Indeed, article 21 of GDPR gives a data subject the right to object at any time to the processing of their personal data, unless the controller can demonstrate "compelling legitimate grounds" for the processing to override the data subject's rights. In conjunction, article 22 prevents data subjects from being subject to a decision based solely on automated processing that has significant effects, except in a few circumstances, including when it is based on explicit consent and does not rely on special categories of data. In all cases where automated decision making is allowed, suitable measures to safeguard the data subjects' rights and freedoms must also be implemented.

Albeit from different perspectives, stakeholders from techUK to the TUC have emphasised the importance of those articles and of the core principles that they promote. For example, the articles place an element of control in the hands of those that an automated decision affects. They emphasise the need for appropriate safeguards, and they consider the need for a different approach where sensitive data is concerned.

Where the clause adjusts the threshold on automated decision making to unlock innovation, therefore—as the likes of the A-level algorithm scandal and the robo-firings show—it is vital that any changes to regulation maintain and in some cases strengthen the principles set out in articles 21 and 22 of the GDPR. However, as the likes of the Ada Lovelace Institute, Which? and the TUC warn, in reality the Bill does the opposite, watering down existing protections. The amendments I have tabled are designed to rectify that.

2.30 pm

The clause not only amends the threshold on automated decision making so that it is permitted in a far wider range of circumstances, but it defines solely automated processing as a "significant decision" that involves "no meaningful human involvement" and attaches all available safeguards to that definition. Furthermore, crucially, the clause gives the Secretary of State the power to amend what counts within the definition. That means that in a world where more automated decision making will be allowed than ever before, safeguards—including the right to be notified of an automated decision, the ability to contest decisions and the right to seek human intervention—will be applicable only at the whim of however the Secretary of State decides to define key terms.

That may well be reasonable when a well informed Secretary of State acts in good faith, updating a definition to add more clarity or to take into account future developments; but the Bill offers no protections against a Minister acting maliciously or on bad advice, deliberately or inadvertently thinning the definition of these terms, with the effect of excluding many automated decisions from having to offer vital safeguards.

Definitions of terms such as "similarly significant" effects and "meaningful human involvement" have always been important to the application of law around automated decision making, and are core to interpreting article 22. That was demonstrated by the Uber case, where it was clearly judged that there was no meaningful intervention. Under the Bill, it is possible that the likes of those Uber drivers would have no legal grounds to complain about having been automatically fired with no recourse. That is simply not right. If technology is used to make genuinely significant or legal decisions about someone's life or employment, that person must be offered proper methods of redress and recourse. The Secretary of State should absolutely not have the unilateral ability to legislate for definitions that could deny people those rights.

Amendment 76 will ensure that the true impact of any changes to definitions and safeguards are considered, and that the regulator is consulted before any adjustments are made. The ability to future-proof definitions through changes will remain when it is truly needed, but necessary extra safeguards will be put in place, so that assurances that the power will not be abused are based in law, not in trust alone. Any changes deemed to be in the general better interests of the public will be able to go ahead, but confidence will be built in for everyone—from consumers to workers—that the Secretary of State cannot define them out of having the rights they deserve.

Moving on to amendment 75, given the importance of the definitions of "similarly significant" and "meaningful human involvement" to the application of safeguards in any given scenario, it is crucial that as well as preventing the Secretary of State from unnecessarily changing the definitions, we ensure that both controllers and the general public are clear on what falls within the definitions

at any given point. The likes of the Public Law Project, the TUC, Which? and the Ada Lovelace Institute have all pointed that out, partly out of a need for general clarity, but also out of a fear that controllers may be able to use loose definitions to define their decision-making activities outside the boundaries of the new articles 22A to 22D, thus preventing the necessary safeguards from applying.

The ICO already offers some brief guidance on the difference between a partly automated and solely automated decision, stating that

> "A process won't be considered solely automated if someone weighs up and interprets the result of an automated decision before applying it to the individual."

The ICO also gives some examples of a significant effect and points toward WP29 guidance on the subject, too. However, the Government make no effort in the Bill or the new rules around automated decision making to indicate that any such clarity or any examples will be provided. That means that, even before the Secretary of State has the power to change the definitions, there may still be confusion on how they apply. Such confusion is unacceptable; it will at best clog up the regulators' time, and at worst cause people to be subject, without proper methods of redress, to automated decisions that have a genuine impact on their lives.

The amendment would build clarity into the Bill by guaranteeing statutory guidance from the Information Commissioner on how the terms are to be applied in practice. In particular, it will clarify the kinds of processing that do not count as falling within these definitions. For example, the guidance could juxtapose examples of meaningful human involvement and rubber stamping, so that controllers would have no excuse to define token gestures as a meaningful intervention. For anyone who wishes to comply with the spirit of the clause, no extra steps will be required; the provision will simply provide greater information to controllers on how to interpret the law, and protect those who are subject to automated decisions.

Sir John Whittingdale: The hon. Lady began her remarks on the broader question of the ambition to ensure that the UK benefits to the maximum extent from the use of artificial intelligence. We absolutely share that ambition, but also agree that it needs to be regulated. That is why we have published the AI regulation White Paper, which suggests that it is most appropriate that each individual regulator should develop its own rules on how that should apply. I think in the case that she was quoting of those who had lost their jobs, maybe through an automated process, the appropriate regulator—in that case, presumably, the special employment tribunal—would need to develop its own mechanism for adjudicating decisions.

I will concentrate on the amendment. On amendment 76, we feel that clause 44 already provides for an overarching requirement on the Secretary of State to consult the Information Commissioner and other persons that she or he considers appropriate before making regulations under UK GDPR, including the measures in article 22. When the new clause 44 powers are used in reference to article 22 provisions, they will be subject to the affirmative procedure in Parliament. I know that the hon. Lady is not wholly persuaded of the merits of using the affirmative procedure, but it does mean that parliamentary approval will be required. Given the level of that scrutiny, we do not think it is necessary for the Secretary of State to have to publish an assessment, as the hon. Lady would require through her amendment.

On amendment 75, as we have already debated in relation to previous amendments, there are situations where non-statutory guidance, which can be produced without being requested under regulations made by the Secretary of State, may be more appropriate than a statutory code of practice. We believe that examples of the kinds of processing that do and do not fall within the definitions of the terms "meaningful human involvement" and "similarly significant" are best placed in non-statutory guidance produced by the ICO, as this will give the flexibility to amend and change the examples where necessary. What constitutes a significant decision or meaningful human involvement is often highly context-specific, and the current wording allows for some interpretability to enable the appropriate application of this provision in different contexts, rather than introducing an absolute definition that risks excluding decisions that ought to fall within this provision and vice versa. For that reason, we are not minded to accept the amendments.

Stephanie Peacock: I appreciate the Minister's remarks about consultation and consulting relevant experts. He is right to observe that I am not a big fan of the affirmative procedure as a method of parliamentary scrutiny but I appreciate that it is included in this Bill as part of that.

I think the problem is that we fundamentally disagree on the power to change these definitions being concentrated in the hands of the Secretary of State. It is one thing to future-proof the Bill but another to allow the Secretary of State alone to amend things as fundamental as the safeguards offered here. I would therefore like to proceed to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 10.

Division No. 13]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

Question accordingly negatived.

Amendment proposed: 75, clause 11, page 19, line 36, at end insert—

> '7. The Commissioner must prepare a code of practice under section 124A of the Data Protection Act 2018 on the interpretation of references in this Regulation to "meaningful human involvement" and "similarly significant".
>
> 8. The code of practice prepared under paragraph 7 must include examples of the kinds of processing which do, and which do not, fall within the definitions which use the terms referred to in that paragraph.' —*(Stephanie Peacock.)*

This amendment would require the ICO to produce a code of practice on the interpretation of references to "meaningful human involvement" and "similarly significant" in connection with automated decision-making, with examples of the kinds of processing that would not count as falling within these definitions.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 10.

Division No. 14]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

Question accordingly negatived.

Stephanie Peacock: I beg to move amendment 121, in clause 11, page 19, line 36, at end insert—

"7. When exercising the power to make regulations under this Article, the Secretary of State must have regard to the following statement of principles:

Digital information principles at work

1. People should have access to a fair, inclusive and trustworthy digital environment at work.

2. Algorithmic systems should be designed and used to achieve better outcomes: to make work better, not worse, and not for surveillance. Workers and their representatives should be involved in this process.

3. People should be protected from unsafe, unaccountable and ineffective algorithmic systems at work. Impacts on individuals and groups must be assessed in advance and monitored, with reasonable and proportionate steps taken.

4. Algorithmic systems should not harm workers' mental or physical health, or integrity.

5. Workers and their representatives should always know when an algorithmic system is being used, how and why it is being used, and what impacts it may have on them or their work.

6. Workers and their representatives should be involved in meaningful consultation before and during use of an algorithmic system that may significantly impact work or people.

7. Workers should have control over their own data and digital information collected about them at work.

8. Workers and their representatives should always have an opportunity for human contact, review and redress when an algorithmic system is used at work where it may significantly impact work or people. This includes a right to a written explanation when a decision is made.

9. Workers and their representatives should be able to use their data and digital technologies for contact and association to improve work quality and conditions.

10. Workers should be supported to build the information, literacy and skills needed to fulfil their capabilities through work transitions."

This amendment would insert into new Article 22D of the UK GDPR a requirement for the Secretary of State to have regard to the statement of digital information principles at work when making regulations about automated decision-making.

The Chair: With this it will be convenient to discuss amendment 122, in clause 11, page 22, line 2, at end insert—

"(7) When exercising the power to make regulations under this section, the Secretary of State must have regard to the following statement of principles:

Digital information principles at work

1. People should have access to a fair, inclusive and trustworthy digital environment at work.

2. Algorithmic systems should be designed and used to achieve better outcomes: to make work better, not worse, and not for surveillance. Workers and their representatives should be involved in this process.

3. People should be protected from unsafe, unaccountable and ineffective algorithmic systems at work. Impacts on individuals and groups must be assessed in advance and monitored, with reasonable and proportionate steps taken.

4. Algorithmic systems should not harm workers' mental or physical health, or integrity.

5. Workers and their representatives should always know when an algorithmic system is being used, how and why it is being used, and what impacts it may have on them or their work.

6. Workers and their representatives should be involved in meaningful consultation before and during use of an algorithmic system that may significantly impact work or people.

7. Workers should have control over their own data and digital information collected about them at work.

8. Workers and their representatives should always have an opportunity for human contact, review and redress when an algorithmic system is used at work where it may significantly impact work or people. This includes a right to a written explanation when a decision is made.

9. Workers and their representatives should be able to use their data and digital technologies for contact and association to improve work quality and conditions.

10. Workers should be supported to build the information, literacy and skills needed to fulfil their capabilities through work transitions."

This amendment would insert into new section 50D of the DPA2018 a requirement for the Secretary of State to have regard to the statement of digital information principles at work when making regulations about automated decision-making.

Stephanie Peacock: Amendments 121 and 122 would ensure that close attention is paid to the specific and unique circumstances of workers and the workplace when regulations are made under the clause. Indeed, as has already been referenced, the workplace has dramatically evolved in the last decade with the introduction and growth of technology. Whether it be Royal Mail using the postal digital assistant service to calculate the length of time posties spend walking, on doorsteps and standing still, or Amazon collecting data from handheld scanners to calculate how much time workers are spending "off task", the digital monitoring of workers and subsequent use of that data by managers to assess performance, allocate work hours and decide on levels of pay, is on the rise.

Of course it is absolutely right that workplaces embrace technology. As Andrew Pakes of Prospect said to this Committee, our economy and the jobs that people do each day can be made better and more productive through the good deployment of technology—but the key is in the phrase "good deployment", and in order to have deployment that works for the greater good, the rights and protections in place at work must keep pace with the changing nature of the workplace and these technological advancements. As Labour outlined in our

[Stephanie Peacock]

industrial strategy, we want to do just that: harness data for the public good and ensure that data and the innovation it brings with it benefit our wider society, not just large corporations. Further, as is written in our "New Deal for Working People", Labour wants to introduce new rights to protect workers in the modern age—for example by legislating to make proposals to introduce surveillance technologies subject to consultation and agreement of trade unions, or elected staff representatives where there is no trade union. After all, we can only truly unlock the benefits of data and become a world leader in this space if there is genuine public trust in these technologies. Good regulation breeds that trust.

Currently, however, and particularly in the Bill, the kinds of measures that would allow for good deployment of technology in the workplace—technology that operates in the greater interest including that of workers—are missing from the Government's plans. Instead, as the TUC note, we are overseeing a growing power imbalance between worker and employer. This imbalance not only exists by the nature of the relationship, but it is now being exacerbated by the increasing level of knowledge and control that employers have over personal data as the workplace becomes digitised, compared with workers, who have very little power over, expertise on or access to such data.

Some impressive projects have sought to address that imbalance. For example, in 2020 Prospect worked with a coalition of unions, tech specialists and researchers to launch a beta version of WeClock, a free mobile app that helps workers to track and manage their own data such as that related to their location, their commute and when they are doing work on their phone. Those data profiles could then potentially be used by trade union campaigners to improve rights for workers. However, it should not just be down to individual projects to ensure that there is an equal balance between worker and employer. The Bill is a huge missed opportunity to write into law this balance and the principles that we should consider with regard to worker's rights in the modern age.

The amendment, which has been prepared in partnership with the Institute for the Future of Work, is designed to right that wrong and ensure that where regulations are made about automated decision making, the full impact on workers is considered and strong principles about worker involvement are upheld. It will mean that the Secretary of State has to consider that people have an inclusive digital environment at work, that they should be protected from harms by algorithmic systems, and that they should be meaningfully consulted before and after the use of such tools. Further, under this amendment, consideration will be given to supporting workers in building the information, literacy and skills needed to understand these transitions in the workplace, thereby addressing some of the imbalances in knowledge and understanding.

I will end with an example of the real-life consequences of employment and data laws lagging behind technology. As was revealed by a report by the Worker Info Exchange just last month, 11 Just Eat couriers in the UK were recently robotically fired after receiving allegations of fraudulent activity identified by an automated system. According to the report, these workers were falsely accused of receiving "undeserved financial gain" relating to nominal waiting time payments at restaurants. Just Eat argued that the workers left the restaurant while continuing to claim waiting fees. However, GPS evidence showed that workers had stayed in the vicinity of the restaurant, usually in the car park. In each case, the worker collected the food and completed the delivery, and the average value of the alleged undeserved payments justifying the robo-firings was just £1.44. Cases such as those, in which real livelihoods are impacted and rights infringed for the sake of profit margins, can and must be avoided.

The amendment would take the first steps in ensuring that regulations around automated decision making centre the unique experience of workers. It also highlights the Bill's failure to move towards a legislative framework in which a distinct focus is placed on harnessing data for the public good, which is something that Labour would have placed at the heart of a data Bill such as this one.

2.45 pm

Chi Onwurah: I rise to speak briefly in support of the amendment tabled by my hon. Friend the Member for Barnsley East and to emphasise the points that she made regarding the importance of putting forward a vision for the protection of workers as the nature of working environments change. That is part of what the amendment's "digital information principles at work" seek to do. I declare an interest: I worked for Ofcom as head of technology before coming to this House. That work highlighted to me the importance of forward-looking regulation. As my hon. Friend set out, artificial intelligence is not forward looking; it is here with us and in the workplace.

Many technological changes have made work more accessible to more people: covid showed us that we could work from many different locations—indeed, Parliament successfully worked from many locations across the country. Technological changes have also made work more productive, and companies and public sector organisations are taking advantage of that increase in productivity. But some technologies have accelerated bad employment practices, driven down standards and damaged the wellbeing of workers—for example, workplace surveillance technologies such as GPS tracking, webcam monitoring and click monitoring, which encroach on workers' privacy and autonomy. My constituents often say that they feel that technology is something that is done to them, rather than something that has their consent and empowers them.

It is important, as I am sure that the Minister will agree, that working people welcome and embrace the opportunities that technology can bring, both for them and for the companies and organisations they work for, but that cannot happen without trust in those technologies. For that, there need to be appropriate regulation and safeguards. Surely the Minister must therefore agree that it is time to bring forward a suite of appropriate principles that follows amendment's principle of

"a fair, inclusive and trustworthy digital environment at work."

I hope that he cannot disagree with any of that.

If we are to get ourselves out of the economic stagnation and lack of growth of the last 10 or 13 years, we need to build on new technologies and productivity, but we

cannot do that without the support and trust of people in the workforce. People must feel that their rights—new rights that reflect the new environment in the workplace—are safeguarded. I hope that the Minister will agree that the principles set out in the amendment are essential to building that trust, and to ensuring a working environment in which workers feel protected and able to benefit from advances in technology.

Sir John Whittingdale: I am grateful to the hon. Members for Barnsley East and for Newcastle upon Tyne Central for setting out the thinking behind the amendment. We share the view, as the hon. Member for Newcastle upon Tyne Central has just said, that those who are subject to artificial intelligence and automated decision making need to have trust in the process, and there need to be principles underlying the way in which those decisions are taken. In each case, the contributions go above and beyond the provision in the Bill. On what we are proposing regarding data protection, the changes proposed in clause 11 will reinforce and provide further clarification, as I have said, in respect of the important safeguards for automated decision making, which may be used in some workplace technologies. These safeguards ensure that individuals are made aware of and can seek human intervention on significant decisions that are taken about them through solely automated means. The reforms to article 22 would make clear employer obligations and employee rights in such scenarios, as we debated in the earlier amendments.

On the wider question, we absolutely recognise that the kind of deployment of technology in the workplace shown in the examples that have already been given needs to be considered across a wide range of different regulatory frameworks in terms of not just data protection law, but human rights law, legal frameworks regarding health and safety and, of course, employment law.

Chi Onwurah: I thank the Minister for his comments. I note that he castigates us, albeit gently, for tabling an amendment to this data protection Bill, while he argues that there is a need for wider legislation to enshrine the rights he apparently agrees with. When and where will that legislation come forward? Does he recognise that we waited a long time and listened to similar arguments about addressing online harms, but have ended up in a situation where—in 2023—we still do not have legislation on online harms? My question is: if not now, when?

Sir John Whittingdale: As I was Chair of the Culture, Media and Sport Committee in 2008 when we published a report calling for legislation on online safety, I recognise the hon. Lady's point that these things take a long time—indeed, far too long—to come about. She calls for action now on governance and regulation of the use of artificial intelligence. She will know that last month the Government published the AI regulation White Paper, which set out the proposals for a proportionate outcomes-focused approach with a set of principles that she would recognise and welcome. They include fairness, transparency and explainability, and we feel that this has the potential to address the risks of possible bias and discrimination that concern us all. As she knows, the White Paper is currently out to consultation, and I hope that she and others will take advantage of that to respond. They will have until 21 June to do so.

I assure the hon. Lady and the hon. Member for Barnsley East that the Government are keenly aware of the need to move swiftly, but we want to do so in consultation with all those affected. The Bill looks at one relatively narrow aspect of the use of AI, but certainly the Government's general approach is one that we are developing at pace, and we will obviously respond once the consultation has been completed.

Stephanie Peacock: The power imbalance between employer and worker has no doubt grown wider as technology has developed. Our amendment speaks to the real-life consequences of that, and to what happens when employment and data law lags behind technology. For the reasons that have been outlined by my hon. Friend the Member for Newcastle upon Tyne Central and myself, I would like to continue with my amendment.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 10.

Division No. 15]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

Question accordingly negatived.

Amendment proposed: 122, in clause 11, page 22, line 2, at end insert—

"(7) When exercising the power to make regulations under this section, the Secretary of State must have regard to the following statement of principles:

Digital information principles at work

1. People should have access to a fair, inclusive and trustworthy digital environment at work.

2. Algorithmic systems should be designed and used to achieve better outcomes: to make work better, not worse, and not for surveillance. Workers and their representatives should be involved in this process.

3. People should be protected from unsafe, unaccountable and ineffective algorithmic systems at work. Impacts on individuals and groups must be assessed in advance and monitored, with reasonable and proportionate steps taken.

4. Algorithmic systems should not harm workers' mental or physical health, or integrity.

5. Workers and their representatives should always know when an algorithmic system is being used, how and why it is being used, and what impacts it may have on them or their work.

6. Workers and their representatives should be involved in meaningful consultation before and during use of an algorithmic system that may significantly impact work or people.

7. Workers should have control over their own data and digital information collected about them at work.

8. Workers and their representatives should always have an opportunity for human contact, review and redress when an algorithmic system is used at work where it may significantly impact work or people. This includes a right to a written explanation when a decision is made.

9. Workers and their representatives should be able to use their data and digital technologies for contact and association to improve work quality and conditions.

10. Workers should be supported to build the information, literacy and skills needed to fulfil their capabilities through work transitions." *—(Stephanie Peacock.)*

This amendment would insert into new section 50D of the DPA2018 a requirement for the Secretary of State to have regard to the statement of digital information principles at work when making regulations about automated decision-making.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 10.

Division No. 16]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

Question accordingly negatived.

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

Sir John Whittingdale: We have, I think, covered a lot of ground already in the debates on the amendments. To recap, clause 11 reforms the rules relating to automated decision making in article 22 of the UK GDP and relevant sections of the Data Protection Act 2018. It expands the lawful grounds on which solely automated decision making that produces a legal or similarly significant effect on an individual may be carried out.

Currently, article 22 of the UK GDPR restricts such activity to a narrow set of circumstances. By expanding the available lawful grounds and ensuring we are clear about the required safeguards, these reforms will boost confidence that the responsible use of this technology is lawful, and will reduce barriers to responsible data use.

The clause makes it clear that solely automated decisions are those that do not involve any meaningful human involvement. It ensures that there are appropriate constraints on the use of sensitive personal data for solely automated decisions, and that such activities are carried out in a fair and transparent manner, providing individuals with key safeguards.

The clause provides three powers to the Secretary of State. The first enables the Secretary of State to describe cases where there is or is not meaningful human involvement in the taking of a decision. The second enables the Secretary of State to further describe what is and is not to be taken as having a significant effect on an individual. The third enables the introduction of further safeguards, and allows those already set out in the reforms to be amended but not removed.

The reformed section 50 of the Data Protection Act mirrors the changes in subsection (1) for solely automated decision making by law enforcement agencies for a law enforcement purpose, with a few differences. First, in contrast to article 22, the rules on automated decision making apply only where such decisions have an adverse legal or similarly significant effect on the individual. Secondly, the processing of sensitive personal data cannot be carried out for the purposes of entering into a contract with the data subject for law enforcement purposes.

The final difference relates to the safeguards for processing. This clause replicates the UK GDPR safeguards for law enforcement processing but also allows a controller to apply an exemption to them where it is necessary for a particular reason, such as to avoid obstructing an inquiry. This exemption is available only where the decision taken by automated means is reconsidered by a human as soon as reasonably practicable.

The subsections amending relevant sections of the Data Protection Act 2018, which apply to processing by or on behalf of the intelligence services, clarify that requirements apply to decisions that are entirely automated, rather than solely automated. They also define what constitutes a decision based on this processing. I have explained the provisions of the clause, and hope the Committee will feel able to accept it.

Stephanie Peacock: I talked at length about my views about the changes to automated decision making when we debated amendments 77, 120, 76, 75, 121 and 122. I have nothing further to add at this stage, but those concerns still stand. As such, I cannot support this clause.

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

The Committee divided: Ayes 10, Noes 6.

Division No. 17]

AYES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

NOES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

Question accordingly agreed to.

Clause 11 ordered to stand part of the Bill.

Schedule 3

Automated decision-making: consequential amendments

3 pm

Sir John Whittingdale: I beg to move amendment 17, in schedule 3, page 140, line 9, leave out sub-paragraph (3) and insert—

"(3) In paragraph 2—

(a) for "under Articles 15 to 22", in the first place, substitute "arising under or by virtue of Articles 15 to 22D", and

(b) for "his or her rights under Articles 15 to 22" substitute "those rights".".

This amendment adjusts consequential amendments of Article 12(2) of the UK GDPR for consistency with other amendments of the UK GDPR consequential on the insertion of new Articles 22A to 22D.

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

Government amendments 18 to 23.

That schedule 3 be the Third schedule to the Bill.

Sir John Whittingdale: I can be reasonably brief on these amendments. Schedule 3 sets out the consequential changes needed to reflect references to the rules on automated decision making in reformed article 22 and section 50 and other provisions in the UK GDPR and the Data Protection Act 2018. Schedule 3 also sets out that section 14 of the Data Protection Act is repealed. Instead, reformed article 22 sets out the safeguards that must apply, regardless of the lawful ground on which such activity is carried out.

Government amendments 17 to 23 are minor technical amendments ensuring that references elsewhere in the UK GDPR and the Data Protection Act to the provisions on automated decision making are comprehensively updated to reflect the reforms related to such activity in this Bill. That means that references to article 22 UK GDPR are updated to the reformed article 22A to 22D provisions, and references to sections 49 and 50 in the Data Protection Act are updated to the appropriate new sections 50A to 50D.

Stephanie Peacock: I thank the Minister for outlining these technical changes. I have nothing further to add on these consequential amendments beyond what has already been discussed on clause 11 and the rules around automated decision making. Consistency across the statute book is important, but all the concerns I raised when discussing the substance of those changes remain.

Amendment 17 agreed to.

Amendments made: 18, in schedule 3, page 140, line 30, before second "in" insert "provided for".

This amendment and Amendment 19 adjust consequential amendments of Article 23(1) of the UK GDPR for consistency with other amendments of the UK GDPR consequential on the insertion of new Articles 22A to 22D.

Amendment 19, in schedule 3, page 140, line 31, leave out "in or under" and insert

"arising under or by virtue of".

See the explanatory statement for Amendment 18.

Amendment 20, in schedule 3, page 140, line 33, leave out from "protection" to end of line 35 and insert

"in accordance with, and with regulations made under, Articles 22A to 22D in connection with decisions based solely on automated processing (including decisions reached by means of profiling)".

This amendment adjusts the consequential amendment of Article 47(2)(e) of the UK GDPR to reflect the way in which profiling is required to be taken into account for the purposes of provisions about automated decision-making (see Article 22A(2) inserted by clause 11).

Amendment 21, in schedule 3, page 140, line 36, leave out paragraph 10 and insert—

"10 In Article 83(5) (general conditions for imposing administrative fines)—

(a) in point (b), for "22" substitute "21", and

(b) after that point insert—

"(ba) Article 22B or 22C (restrictions on, and safeguards for, automated decision-making);"".

This amendment adjusts the consequential amendment of Art 83(5) of the UK GDPR (maximum amount of penalty) for consistency with the consequential amendment of equivalent provision in section 157(2) of the Data Protection Act 2018.

Amendment 22, in schedule 3, page 141, line 8, leave out sub-paragraph (2) and insert—

"(2) In subsection (3), for "by the data subject under section 45, 46, 47 or 50" substitute "made by the data subject under or by virtue of any of sections 45, 46, 47, 50C or 50D".".

This amendment adjusts the consequential amendment of section 52(3) of the Data Protection Act 2018 for consistency with other amendments of that Act consequential on the insertion of new sections 50A to 50D.

Amendment 23, in schedule 3, page 141, line 9, leave out sub-paragraph (3) and insert—

"(3) In subsection (6), for "under sections 45 to 50" substitute "arising under or by virtue of sections 45 to 50D"".—*(Sir John Whittingdale.)*

This amendment adjusts the consequential amendment of section 52(6) of the Data Protection Act 2018 for consistency with other amendments of that Act consequential on the insertion of new sections 50A to 50D.

Schedule 3, as amended, agreed to.

Clause 12

General obligations

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

Sir John Whittingdale: One of the main criticisms that the Government have received of the current legislative framework is that it sets out a number of prescriptive requirements that organisations must satisfy to demonstrate compliance. They include appointing independent data protection officers, keeping records of processing, appointing UK representatives, carrying out impact assessments and consulting the ICO about intended processing activities in specified circumstances.

Those rules can sometimes generate a significant and disproportionate administrative burden, particularly for small and medium-sized enterprises and for some third sector organisations. The current framework provides some limited exemptions for small businesses and organisations that are carrying out low-risk processing activities, but they are not always as clear or as useful as they should be.

We are therefore taking the opportunity to improve chapter 4 of the UK GDPR, and the equivalent provisions in part 3 of the Data Protection Act, in respect of law enforcement processing. Those provisions deal with the policies and procedures that organisations and law enforcement organisations must put in place to monitor and ensure compliance. Clauses 12 to 20 will give organisations greater flexibility to implement data protection management programmes that work for their organisations, while maintaining high standards of data protection for individuals.

Clause 12 is technical in nature. It will improve the terminology in the relevant articles of the UK GDPR by replacing the requirement to implement

"appropriate technical and organisational measures".

In its place, data protection risks must be managed with

"appropriate measures, including technical and organisational measures,".

That will give organisations greater flexibility to implement any measures that they consider appropriate to help them manage risks. A similar clarification is made to equivalent parts of the Data Protection Act.

[Sir John Whittingdale]

Clause 13 will remove article 27 of the UK GDPR, ending the requirement for overseas controllers or processors to appoint a representative in the UK where they offer goods or services to, or monitor the behaviour of, UK citizens—

The Chair: Order. I am sorry, Minister, but we are talking about clause 12 at the moment; we will come on to clause 13 later. Have you concluded your remarks on clause 12?

Sir John Whittingdale: I think I have covered the points that I would like to make on clause 12.

Stephanie Peacock: Clause 12 is a set of largely technical amendments to terminology that I hope will provide clarity to data controllers and processors. I have no further comments to make at this stage.

Question put and agreed to.

Clause 12 accordingly ordered to stand part of the Bill.

Clause 13

REMOVAL OF REQUIREMENT FOR REPRESENTATIVES FOR CONTROLLERS ETC OUTSIDE THE UK

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

Sir John Whittingdale: As I was saying, clause 13 will remove article 27 of the UK GDPR, ending the requirement for overseas controllers or processors to appoint a representative in the UK where they offer goods or services to, or monitor the behaviour of, UK citizens. By no longer mandating organisations to appoint a representative, we will be allowing organisations to decide for themselves the best way to comply with the requirements for effective communication. That may still include the appointment of a UK-based representative. The removal of this requirement is therefore in line with the Bill's wider strategic aim of removing unnecessary prescriptive regulation.

Stephanie Peacock: The rules set out in the UK GDPR apply to all those who are active in the UK market, regardless of whether their organisation is based or located in the UK. Article 27 of the UK GDPR currently requires controllers and processors based outside the UK to designate a UK-based representative, unless they process only occasionally without special categories of data, providing an element of proportionality, or are a public authority or body. The idea is that the representative will act on behalf of the controller or processor regarding their UK GDPR compliance and will deal with the ICO and data subjects in that respect, acting as a primary contact for all things data within the country.

The removal of the requirement for a UK representative was not included in the Government's consultation, "Data: a new direction", nor was it even mentioned in their response. As a result, stakeholders have not been given an opportunity to put forward their opinions on this change. I wish to represent some of those opinions so that they are on the record for the Minister and his Department to consider.

Concern among the likes of Lexology, DataRep and Which? relates primarily to the fact that the current requirements for UK-based representatives ensure that UK data subjects can conveniently reach the companies that process their personal data, so that they can exercise their rights under the GDPR. Overseas data handlers may have a different first language, operate in a different time zone or have local methods of contact that are not easily accessible from the UK. Having a UK-based point of contact therefore ensures that data subjects do not struggle to apply the rights to which they are entitled because of the inevitable differences that occur across international borders.

As Lexology has pointed out, the Government's own impact assessment says:

> "There is limited information and data on the benefits of having an Article 27 representative as it is a relatively new and untested requirement and also one that applies exclusively to businesses and organisations outside of the UK which makes gathering evidence very challenging."

By their own admission, then, the Government seem to recognise the challenges in gathering information from organisations outside the UK. If the Government find it difficult to get the information that they require, surely average citizens and data subjects may also face difficulties.

Not only is having a point of contact a direct benefit for data subjects, but a good UK representative indirectly helps data subjects by facilitating a culture of good data protection practice in the organisation that they represent. For example, they may be able to translate complex legal concepts into practical business terms or train fellow employees in a general understanding of the UK GDPR. Such functions may make it less likely that a data subject will need to exercise their rights in the first place.

As well as things being harder for data subjects in the ways I have outlined, stakeholders are not clear about the benefits of removing representatives for UK businesses. For example, the Government impact assessment estimates that the change could save a large organisation £50,000 per year, but stakeholders have said that that figure is an overestimation. Even if the figure is accurate, the saving will apply only to organisations outside the UK and will be made through a loss of employment for those who are actually based in the UK and performing the job.

The question therefore remains: if the clause is not in the interests of data subjects, of UK businesses or of UK-based employees who act as representatives, how will this country actually benefit from the change? I am keen to hear from the Minister on that point.

Sir John Whittingdale: If there are concerns that were not fed in during the consultation period, obviously we will consider them. However, it remains the case that even without the article 27 representative requirement, controllers will have to maintain contact with UK citizens and co-operate with the ICO under other provisions of the UK GDPR. For example, overseas controllers and processors must still co-operate with the ICO as a result of the specific requirements to do so under article 31 of the UK GDPR. To answer the hon. Lady's question

about where the benefit lies, the clause is part of a streamlining process to remove what we see as unnecessary administrative requirements and bureaucracy.

Question put and agreed to.

Clause 13 accordingly ordered to stand part of the Bill.

Clause 14

SENIOR RESPONSIBLE INDIVIDUAL

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

Sir John Whittingdale: As I mentioned in our debate on clause 12, clauses 12 to 18 will give organisations greater flexibility about the policies, procedures or programmes that they put in place to ensure compliance with the legislation. As we have discussed, a criticism of the current legal framework is that many of the existing requirements are so prescriptive that they impose unnecessary burdens on businesses. Many organisations could manage data protection risks effectively without appointing an independent data protection officer, but they are forced to do so by the prescriptive rules that we inherited from the European Union.

Clause 14 will therefore abolish existing requirements on data protection officers and replace them with new requirements for organisations to designate a senior responsible individual where appropriate. That individual would be part of the organisation's senior management and would be responsible for overseeing data protection matters within the organisation. In particular, the individual would be responsible for monitoring compliance with the legislation, ensuring the implementation of appropriate risk management procedures, responding to data protection breaches and co-operating with the information commissioner, or for ensuring that those tasks are performed by another suitably skilled person where appropriate. Senior responsible individuals may perform the tasks specified in clause 14 themselves, delegate them to suitably skilled members of staff or, if it is right for the company and its clients, seek advice from independent data protection experts.

We recognise that some people have raised concerns that giving organisations more flexibility in how they monitor and ensure compliance with the legislation could reduce standards of protection for individuals. We are confident that that will not be the effect of the clause. On the contrary, the clause provides an opportunity to elevate discussions about data protection risks to senior levels within organisations by requiring a senior responsible individual to take ownership of data protection risks and embed a culture of data protection. On that basis, I commend the clause to the Committee.

3.15 pm

Stephanie Peacock: In a number of places in the Bill, the Government have focused on trying to ensure a more proportionate approach to data protection. That often takes the form of reducing regulatory requirements on controllers and processors where low-risk processing, which presents less of a threat of harm to data subjects, is taking place. Clause 14 is one place in which Ministers have applied that principle, replacing data protection officers with a requirement to appoint a senior responsible individual, but only where high-risk processing is being carried out.

Such a proportionate approach makes sense in theory. Where the stakes are lower, less formalised oversight of GDPR compliance will be required, which will be particularly helpful in small business settings where margins and resources are tight. Where the stakes are higher, however, a senior responsible individual will have a similar duty to that of a data protection officer, but with the added benefit of being part of the senior leadership team, ensuring that data protection is considered at the highest level of organisations conducting high-risk processing.

However, the Government have admitted that the majority of respondents to their consultation disagreed with the proposal to remove the requirement to designate a data protection officer. In particular, respondents were concerned that removing DPOs would result in

"a loss of data protection expertise"

and

"a potential fall in trust and reassurance to data subjects."

Indeed, data protection officers perform a vital role in upholding GDPR, taking on responsibility for informing people of their obligations; monitoring compliance, including raising awareness and training staff; providing advice, where requested, on data protection impact assessments; co-operating with the regulator; and acting as a contact point. That provides not only guaranteed expertise to organisations, but reassurance to data subjects that they will have someone to approach should they feel the need to exercise any of their rights under the GDPR.

The contradiction between the theory of the benefits of proportionality and the reality of the concerns expressed by respondents to the consultation emphasises a point that the Government have repeatedly forgotten throughout the Bill: although removing truly unnecessary burdens can sometimes be positive, organisations often want clear regulation more than they want less regulation. They believe in the principles of the GDPR, understand the value of rights to data subjects and often over-comply with regulation out of fear of breaking the rules.

In this context, it makes sense that organisations recognise the value of having a data protection officer. They actually want in-house expertise on data—someone they can ask questions and someone they can rely on to ensure their compliance. Indeed, according to the DPO Centre, in September 2022, the UK data protection index panel of 523 DPOs unequivocally disagreed with the idea that the changes made by the clause would be in the best interests of data subjects. Furthermore, when asked whether the proposal to remove the requirement for a DPO and replace it with a requirement for a senior responsible individual would simplify the management of privacy in their organisation, 42% of DPOs surveyed gave the lowest score of 1.

Did the Department consider offering clarification, support and guidance to DPOs, rather than just removing them? Has it attempted to assess the impact of their removal on data subjects? In practice, it is likely that many data protection officers will be rebranded as senior responsible individuals. However, many will be relieved of their duties, particularly since the requirement to be part of the organisation's senior management

[Stephanie Peacock]

team could be problematic for external DPO appointments and those in more junior positions. Has the Department assessed how many data protection officers may lose their job as a result of these changes? Is the number expected to be substantial? Will there be any protections to support those people in transitioning to skilled employment surrounding data protection and to prevent an overall reduction of data protection expertise in organisations?

Sir John Whittingdale: The clause does not in any way represent a lessening of the requirement on organisations to comply with data protection law. It simply introduces a degree of flexibility. An organisation could not get rid of data protection officers without ensuring that processing activities likely to pose high risks to individuals are still managed properly. The senior responsible individual will be required to ensure that that is the case.

At the moment, even small firms whose core activities do not involve the processing of sensitive data must have a data protection officer. We feel that that is an unnecessary burden on those small firms, and that allowing them to designate an individual will give them more flexibility without reducing the overall level of data protection that they require.

Question put and agreed to.

Clause 14 accordingly ordered to stand part of the Bill.

Clause 15

DUTY TO KEEP RECORDS

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

The Chair: With this it will be convenient to discuss clause 16 stand part.

Sir John Whittingdale: Clauses 15 and 16 will improve the record-keeping requirements under article 30 of the UK GDPR and the logging requirements under part 3 of the Data Protection Act, which is concerned with records kept for law enforcement purposes. Article 30 of the UK GDPR requires most organisations to keep records of their processing activities and includes a list of requirements that should be included in the record. Those requirements can add to the paperwork that organisations have to keep to demonstrate compliance. Although there is an exemption from those requirements in the UK GDPR for some small organisations, it has a limited impact because it applies only where their processing of personal data is "occasional".

Clause 15 will replace the record-keeping requirements under article 30. It will make it easier for data controllers to understand exactly what needs to be included in the record. Most importantly, organisations of any size will no longer have to keep records of processing, unless their activities are

"likely to result in a high risk"

to individuals. That should help small businesses in particular, which have found the current small business exemption difficult to understand and apply in practice.

Clause 16 will make an important change to the logging requirements for law enforcement purposes in part 3 of the Data Protection Act. It will remove the ineffective requirement to record a justification when an officer consults or discloses personal data for the purposes of an investigation. The logging requirements are unique to the law enforcement regime and aim to assist in monitoring and auditing data use. Recording a justification for accessing data was intended to help protect against unlawful access, but the reality is that someone is unlikely to record an honest reason if their access is unlawful. That undermines the purpose of this requirement, because appropriate and inappropriate uses would both produce essentially indistinguishable data.

As officers often need to access large amounts of data quickly, especially in time-critical scenarios, the clause will facilitate the police's ability to investigate and prevent crime more swiftly. We estimate that the change could save approximately 1.5 million policing hours. Other elements of the logs, such as the date and time of the consultation or disclosure and the identity of the person accessing them, are likely to be far more effective in protecting personal data against misuse; those elements remain in place. On that basis, I commend the clauses to the Committee.

Stephanie Peacock: Record keeping is a valuable part of data processing. It requires controllers, and to a lesser extent processors, to stay on top of all the processing that they are conducting by ensuring that they record the purposes for processing, the time limits within which they envisage holding data and the categories of recipients to whom the data has been or will be disclosed.

Many respondents to the Government's consultation "Data: a new direction" said that they did not think the current requirements were burdensome. In fact, they said that the records allow them easily to understand the personal data that they are processing and how sensitive it is. It is likely that that was helped by the fact that the requirements were proportionate, meaning that organisations that employed under 250 people and were not conducting high-risk processing were exempt from the obligations.

It is therefore pleasing to see the Government rolling back on the idea of removing record-keeping requirements entirely, as was suggested in their consultation. As was noted, the majority of respondents disagreed with that proposal, and it is right that it has been changed. However, some respondents indicated a preference for more flexibility in the record-keeping regime, which is what I understand the clause is trying to achieve. Replacing the current requirements with a requirement to keep an appropriate record of processing, tied to high-risk activities, will give controllers the flexibility that they require.

As with many areas of the Bill, it is important that we be clear on the definition of "appropriate" so that it cannot be used by those who simply do not want to keep records. I therefore ask the Minister whether further guidance will be available to assist controllers in deciding what counts as appropriate.

I also wish to highlight the point that although in isolation the clause does not seem to change requirements much, other than by adding an element of proportionality, it cannot be viewed in isolation. In combination with other provisions, such as the reduced requirements on

DPIAs and the higher threshold for subject access requests, it seems that there will be less records overall on which a data subject might be able to rely to understand how their personal information is being used or to prove how it has been used when they seek redress. With that in mind, I ask the Minister whether the Government have assessed the potential impact of the combination of the Bill's clauses on the ability of data subjects to exercise their rights. Do the Government have any plans to work with the commissioner to monitor any such impacts on data subjects after the Bill is passed?

I turn to clause 16. Section 62 of the Data Protection Act 2018 requires competent authorities to keep logs that show who has accessed certain datasets, and at what time. It also requires that that access be justified: the reason for consulting the data must be given. Justification logs exist to assist in disciplinary proceedings, for example if there is reason to believe that a dataset has been improperly accessed or that personal data has been disclosed in an unauthorised way. However, as Aimee Reed, director of data at the Met police and chair of the national police data board, told the Committee:

"It is a big requirement across all 43 forces, largely because…we are operating on various aged systems. Many of the technology systems…do not have the capacity to log section 62 requirements, so police officers are having to record extra justification in spreadsheets alongside the searches".—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 56, Q118.]

That creates what she described as a "considerable burden".

Understandably, therefore, the Bill removes the justification requirement. There are some—the Public Law Project, for example—who have expressed concern that this change would pose a threat to individual rights by allowing the police to provide a retrospective justification for accessing records. However, as the explanatory notes indicate, it is highly unlikely that in an investigation concerning inappropriate use, a justification recorded by the individual under investigation for improper access or unauthorised access could be relied on anyway. Clause 16 would therefore not stop anyone from being investigated for improper access; it would simply reduce the burden of recording a self-identified justification that could hardly be relied on anyway. I welcome the intent of the clause and the positive impact that it could have on our law enforcement processing.

Sir John Whittingdale: The intention behind clause 15 is to reduce the burden on organisations by tying the record-keeping requirements to high-risk processing activities. If there is uncertainty about the nature of the risk, organisations will be able to refer to ICO guidance. The ICO has already published examples on its website of processing that is likely to be high-risk for the purposes of completing impact assessments; clause 17 will require it to apply the guidance to the new record-keeping requirements as well. It will continue to provide guidance on the matter, and we are happy to work with it on that.

With respect to clause 16, I am most grateful for the Opposition's welcome recognition of the benefits for crime prevention and law enforcement.

Question put and agreed to.

Clause 15 accordingly ordered to stand part of the Bill.

Clause 16 ordered to stand part of the Bill.

Clause 17

ASSESSMENT OF HIGH RISK PROCESSING

Stephanie Peacock: I beg to move amendment 102, in clause 17, page 32, line 12, leave out from "with" to the end of line 28 on page 33 and insert

"subsection (2)

(2) In Article 57(1) (Information Commissioner's tasks), for paragraph (k) substitute—

'(k) produce and publish a document containing examples of types of processing which the Commissioner considers are likely to result in a high risk to the rights and freedoms of individuals (for the purposes of Articles 27A, 30A and 35);'."

This amendment would remove the provisions of clause 17 which replace the existing data protection impact assessment requirements with new requirements about "high risk processing", leaving only the requirement for the ICO to produce a document containing examples of types of processing likely to result in a high risk to the rights and freedoms of individuals.

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

Amendment 103, in clause 17, page 33, line 9, at end insert—

"(4A) After Article 35(11) insert—

'(11A) Any public authority, government department, or contractor of a government department which routinely uses public data in the discharge of its functions must publish any assessments of high risk processing conducted pursuant to this Article. Any assessments published under this Article must be redacted where necessary for the purposes of—

(a) removing sensitive details,

(b) protecting public interests, or

(c) ensuring the security of data processing operations.'"

This amendment inserts a new requirement into Article 35 of UKGDPR, for any public authority which uses public data to publish any assessment of high risk processing they conduct under Article 35.

Clause stand part.

Clause 18 stand part.

3.30 pm

Stephanie Peacock: As was the intention, the Bill loosens restrictions on processing personal data in many areas: it adds a new lawful basis and creates new exceptions to purpose limitation, removes blocks to automated decision-making and allows for much thinner record keeping. Each change in isolation may make only a relatively small adjustment to the regime. Collectively, however, they result in a large-scale shift towards controllers being able to conduct more processing, with less transparency and communication, and having fewer records to keep, all of which reduces opportunities for accountability.

As mentioned, loosening restrictions is an entirely deliberate consequence of a Bill that seeks to unlock innovation through data—an aim that Members across the House, including me, are strongly behind, given the power of data to influence growth for the public good. However, given the cumulative impact of this deregulation, where increasingly opaque processing is likely to result in a large risk to people's rights, a processor might at the very least record how they will ensure that any high-risk

[Stephanie Peacock]

activities that they undertake do not lead to unlawful or discriminatory outcomes for the general public. That is exactly what the current system of DPIAs, as outlined in article 35 of GDPR, allows for. These assessments, which require processors to measure their activities against the risk to the rights and freedoms of data subjects, are not just a tick-box exercise, unnecessary paperwork or an administrative burden; they are an essential tool for ensuring that organisations do not deploy, and individuals are not subjected to, systems that may lead to a fundamental breach of their rights.

Assessments of that kind are not a concept unique to data processing. The Government routinely publish impact assessments on the legislation that they want to introduce; any researcher or scientist is likely to conduct an assessment of the safety and morality of their methodology; and a teacher will routinely and formally measure the risks involved when taking pupils on a school trip. Where activities pose a high risk to others, it is simply common practice to keep a record of where the risks lie, and to make plans to ensure that they are mitigated where possible.

In the case of data, not only are DPIAs an important mechanism to ensure that risks are managed, but they act as a key tool for data subjects. That is first because the process of conducting a DPIA encourages processors to consult data subjects, either directly or through a representative, on how the type of processing might impact them. Secondly, where things go wrong for data subjects, DPIAs act as a legal record of the processing, its purpose and the risks involved. Indeed, the Public Law Project, a registered charity that employs a specialist lawyer to conduct research, provide training and take on legal casework, identified DPIAs as a key tool in litigating against the unlawful use of data processing. They show a public law record of the type of processing that has been conducted, and its impact.

The TUC and the Institute for the Future of Work echo that, citing DPIAs as a crucial process and consultation tool for workers and trade unions in relation to the use of technology at work. The clause, however, seeks to water down DPIAs, which will become "assessments of high-risk processing". That guts both the fundamental benefit of risk management that they offer in a data protection system that is about to become increasingly transparent, and the extra benefits that they give to data subjects.

Instead of requiring a systematic description of the processing operations and purposes, under the new assessments the controller would be required only to summarise the purpose of the processing. Furthermore, instead of conducting a proportionality assessment, controllers will be required only to consider whether the processing is necessary for the stated purpose. The Public Law Project describes the proportionality assessment as a crucial legal test that weighs up whether an infringement of human rights, including the right not to be discriminated against, is justified in relation to the processing being conducted.

When it comes to consultation, where previously it was encouraged for controllers to seek the views of those likely to be impacted by the processing, that requirement to seek those views will now be entirely omitted, despite the important benefit to data subjects, workers and communities. The new tests therefore simply do not carry the same weight or benefit as DPIAs, which in truth could themselves be strengthened. It is simply not appropriate to remove the need to properly assess the risk of processing, while simultaneously removing restrictions that help to mitigate those risks. For that reason, the clause must be opposed; we would keep only the requirement for the ICO to produce that much-needed guidance on what constitutes high-risk processing.

Moving on to amendment 103, given the inherent importance of conducting risk assessments for high-risk processing, and their potential for use by data subjects when things go wrong, it seems only right that transparency be built into the system where it comes to Government use of public data. The amendment would do just that, and only that. It would not adjust any of the requirements on Government Departments or public authorities to complete high-risk assessments; it would simply require an assessment to be published in any case where one is completed. Indeed, the ICO guidance on DPIAs says:

> "Although publishing a DPIA is not a requirement of UK GDPR, you should actively consider the benefits of publication. As well as demonstrating compliance, publication can help engender trust and confidence. We would therefore recommend that you publish your DPIAs, where possible, removing sensitive details if necessary."

However, very few organisations choose to publish their assessments. This is a chance for the Government to lead by example, and foster an environment of trust and confidence in data protection

Alongside the amendment I tabled on compulsory reporting on the use of algorithms, this amendment is designed to afford the general public honesty and openness on how their data is used, especially where the process has been identified as having a high risk of causing harm. Again, a published impact assessment would provide citizens with an official record of high-risk uses of their data, should they need that when seeking redress. However, a published impact assessment would also encourage responsible use of data, so that redress does not need to be sought in the first place.

The Government need not worry about the consequences of the amendment if they already meet the requirement to conduct the correct impact assessments and process them in such a way that the benefits are not heavily outweighed by a risk to data rights. If rules are being followed, the amendment will only provide proof of that. However, if anyone using public data in a public authority's name did so without completing the appropriate assessments, or processed that data in a reckless or malicious way, there would be proof of that. Where there is transparency, there is accountability, and where the Government are involved, accountability is always crucial in a democracy. The amendment would ensure that accountability shined through in data protection law.

Finally, I turn to clause 18. The majority of respondents to the "Data: a new direction" consultation agreed that organisations are likely to approach the ICO voluntarily before commencing high-risk processing activities if that is taken into account as a mitigating factor in any future investigation or enforcement action. The loosening of requirements in the clause is therefore not a major concern. However, when that is combined with the watering down of the impact assessments, there remains an overarching concern about the oversight of high-risk

processing. I refer to my remarks on clause 17, in which I set out the broader problems that the Bill poses to protection against harms from high-risk processing.

Sir John Whittingdale: As we have discussed, one of the principal objectives of this part of the Bill is to remove some of the prescriptive unnecessary requirements on organisations to do things to demonstrate compliance. Clauses 17 and 18 reduce the unnecessary burdens placed on organisations by articles 35 and 36 of the UK GDPR in respect of data protection impact assessments and prior consultation with the ICO respectively.

Clause 17 will replace the EU-derived notion of a data protection impact assessment with more streamline requirements for organisations to document how they intend to assess and mitigate risks associated with high-risk processing operations. The changes will apply to both the impact assessment provisions under the UK GDPR and the section of the Data Protection Act 2018 that deals with impact assessments for processing relating to law enforcement. Amendment 102 would reverse those changes to maintain the current data protection impact assessment requirements, but we feel that this would miss an important opportunity for reform.

There are significant differences between the new provisions in the Bill and current provisions on data protection impact assessments. First, the new provisions are less prescriptive about the precise processing activities for which a risk assessment will be required. We think organisations are best placed to judge whether a particular activity poses a high risk to individuals in the context of the situation, taking account of any relevant guidance from the regulator.

Secondly, we have also removed the mandatory requirement to consult individuals about the intended processing activity as part of a risk-assessment process, as that imposes unnecessary burdens. There are already requirements in the legislation to ensure that any new processing is fair, transparent and designed with the data protection principles in mind. It should be open to businesses to consult their clients about intended new processing operations if they wish, but that should not be dictated to them by the data protection legislation.

Clause 18 will make optional the previous requirement for data controllers to consult the commissioner when a risk assessment indicates a potential high risk to individuals. The Information Commissioner will be able to consider any voluntary actions that organisations have taken to consult the ICO as a factor when imposing administrative fines on a data controller. Currently, compliance with the prior consultation requirement is low, likely due to a lack of clarity in the legislation and a reluctance for organisations to engage directly with the regulator on potential high-risk processing. The clause will encourage a more proactive, open and collaborative dialogue between the ICO and organisations, so that they can work together to better mitigate the risks.

The Opposition's amendment 103 would mandate the publication of risk assessments by all public sector bodies. That requirement would, in our view, place a disproportionate burden on public authorities of all sizes. It would apply not just to Departments but to smaller public authorities such as schools, hospitals, independent pharmacies and so on. The amendment acknowledges that each public authority would have to spend time redacting sensitive details from risk assessments prior to publication. As those assessments can already be requested by the ICO as part of its investigations, or by members of the public via freedom of information requests, we do not think it is necessary to impose that significant new burden on all public bodies. I therefore invite the hon. Member for Barnsley East to withdraw her two amendments, and I commend clauses 17 and 18 to the Committee.

Stephanie Peacock: I am happy not to press amendment 103 to a vote, but on amendment 102, I simply do not think it is appropriate to remove the need to properly assess the risk of processing while removing the restrictions that help to mitigate it. For those reasons, I will press it to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 10.

Division No. 18]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

Question accordingly negatived.

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

The Committee divided: Ayes 10, Noes 6.

Division No. 19]

AYES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

NOES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

Question accordingly agreed to.

Clause 17 ordered to stand part of the Bill.

Clause 18 ordered to stand part of the Bill.

Clause 19

Law enforcement processing and codes of conduct

Sir John Whittingdale: I beg to move amendment 1, in clause 19, page 35, leave out lines 23 to 25 and insert—

"(5) The Commissioner must encourage expert public bodies to submit codes of conduct described in subsection (1) to the Commissioner in draft.".

This amendment replaces a duty on expert public bodies to submit draft codes of conduct relating to compliance with Part 3 of the Data Protection Act 2018 to the Information Commissioner with a duty on the Information Commissioner to encourage such bodies to do so.

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

Government amendments 2 to 4.

Clause stand part.

3.45 pm

Sir John Whittingdale: Clause 19 introduces an ability for public bodies with the appropriate knowledge and expertise to produce codes of conduct applicable to the law enforcement regime. The clause mirrors the equivalent provision in the UK GDPR.

As with regular guidance, these codes of conduct will be drafted by law enforcement data protection experts and tailored to the specific data protection issues that affect law enforcement agencies, to help improve compliance with the legislation and encourage best practice. However, they are intended to carry more weight, because they will additionally have the formal approval of the Information Commissioner.

When a code of conduct is produced, there is a requirement to submit a draft of it to the Information Commissioner. While that is good practice, we think it is unnecessary to mandate that. Government amendment 1 replaces that requirement with a duty on the commissioner to instead encourage public bodies to do that. Government amendments 2 and 3 are consequential to that.

Where a public body has submitted a code of conduct to the commissioner for review, Government amendment 4 removes the requirement for the commissioner to review any subsequent amendments made by the public body until the initial draft has been considered. This change will promote transparency, greater clarity and confidence in how police process personal data under the law enforcement regime. Codes of conduct are not a new concept. The clause mirrors what is already available under the UK GDPR.

Stephanie Peacock: The Bill fails to fully recognise that the burdens that organisations face in complying with data protection legislation are not always best dealt with by simply removing the protections in place. In many cases, clarification and proper guidance can be just as fruitful in allowing data protection to work more seamlessly. Clauses such as clause 19, which seeks to create an environment in which best practice is shared on how to comply with data protection laws and deal with key data protection challenges, are therefore very welcome. It is absolutely right that we should capitalise on pockets of experience and expertise, especially in the public sector, where resources have often been stretched, particularly over the last 13 years. We should ensure that learnings are shared with those who are less familiar with how to resolve challenges around data.

It is also pleasing to see that codes that give sector-specific guidance will be approved by the commissioner before being published. That will ensure absolute coherence between guidance and the enforcement of data protection law more widely. I look forward to seeing what positive impact the codes of conduct will have on how personal data is handled by public bodies, to the benefit of the general public as well as the public bodies themselves; the burden on them will likely be lifted as a result of the clarity provided by the guidance.

Sir John Whittingdale: I welcome the Opposition's support.

Amendment 1 agreed to.

Amendments made: 2, in clause 19, page 35, line 26, leave out from 'body' to ', the' in line 27 and insert 'does so'.

This amendment is consequential on Amendment 1.

Amendment 3, in clause 19, page 35, line 28, leave out 'draft'.

This amendment is consequential on Amendment 2.

Amendment 4, in clause 19, page 35, line 33, leave out from 'conduct' to the end of line 34 and insert—

'that is for the time being approved under this section as they apply in relation to a code'.—(*Sir John Whittingdale*.)

This amendment makes clear that the Commissioner's duty under new section 68A of the Data Protection Act 2018 to consider whether to approve amendments of codes of conduct relates only to amendments of codes that are for the time being approved under that section.

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

Clause 20

OBLIGATIONS OF CONTROLLERS AND PROCESSORS: CONSEQUENTIAL AMENDMENTS

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

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

Government amendments 42 and 43.

That schedule 4 be the Fourth schedule to the Bill.

Government amendments 40 and 41.

Sir John Whittingdale: As clauses 12 to 18 remove terms such as data protection officers and data protection impact assessments from the legislation, some consequential changes are required to other parts of the legislation where the same terms are used. Clause 20 therefore introduces schedule 4, which sets out the details of the consequential changes required. An example of that is in article 13 of the UK GDPR, which currently requires controllers to provide individuals with the contact details of the data protection officer, where appropriate. In future, that provision will refer to the organisation's senior responsible individual instead. Removal of the term data protection officer from the UK GDPR will have knock-on effects in other areas, including in relation to the types of people from whom the ICO receives requests and queries.

Government amendment 40 will provide that the commissioner may refuse to deal with vexatious or excessive requests made by any person, not just those made by data protection officers or data subjects. Government amendments 41 to 43 make further minor and technical changes to the provisions in schedule 4 to reflect the changes we have made to the terminology.

Stephanie Peacock: I have no comments to add on the consequential amendments in clause 20 beyond what has been discussed regarding the obligations on controllers and processors. With regard to Government amendments 40 to 44 and schedule 4, I will address changes to the ICO's powers to refuse requests when we come to them further on in the Bill.

Question put and agreed to.

Clause 20 accordingly ordered to stand part of the Bill.

Schedule 4

OBLIGATIONS OF CONTROLLERS AND PROCESSORS: CONSEQUENTIAL AMENDMENTS

Amendments made: 42, in schedule 4, page 143, line 20, leave out 'and section 135'.—(*Sir John Whittingdale*.)

This amendment is consequential on Amendment 40.

Amendment 43, in schedule 4, page 143, line 24, leave out paragraph 18.

This amendment is consequential on Amendment 40.

Schedule 4, as amended, agreed to.

Clause 21

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES AND INTERNATIONAL ORGANISATIONS

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

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

Amendment 104, in schedule 5, page 144, line 28, at end insert—

'4 All provisions in this Chapter must be applied in such a way as to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.'

This amendment would reinsert into the new Article on general principles for international data transfers the principle that all provisions of this Chapter of the UK GDPR should be applied in such a way as to ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined.

Government amendments 24 to 26.

That schedule 5 be the Fifth schedule to the Bill.

Government amendments 27 to 29.

That schedule 6 be the Sixth schedule to the Bill.

That schedule 7 be the Seventh schedule to the Bill.

Sir John Whittingdale: Clause 21 refers to schedules 5 to 7, which introduce reforms to the provisions of the UK GDPR and the Data Protection Act 2018, which regulate the international transfers of personal data. Schedule 5 introduces changes to the UK's general processing regime for transferring personal data internationally. In order to provide for a clearer structure than the current UK regime, schedule 5 will consolidate the existing provisions on international transfers. It replaces article 44 with article 44A, setting out in clearer terms the general principles for international transfers and listing the same bases under which personal data can be lawfully transferred overseas.

Schedule 5 also introduces article 45A, which sets out the Secretary of State's power to make regulations approving transfers of personal data to a third country or international organisation. The Government now use the term "data bridges" to refer to those regulations, which allow the free flow of personal data. Article 45A outlines that the Secretary of State may make such regulations only if they are satisfied that the data protection test is met. In addition to the requirement that the Secretary of State be satisfied that the data protection test is met, article 45A specifies that the Secretary of State may have regard to other matters that he or she considers relevant when making those regulations, including the desirability of facilitating transfers of personal data to and from the UK.

Article 45B sets out the data protection test that the Secretary of State must consider is met in order to establish new data bridges. In order for a country or international organisation to meet the data protection test, the standard of protection for personal data in that country or international organisation must be "not materially lower" than the standard of protection under the UK's data protection framework. The reformed law recognises that the Secretary of State must exercise their judgment when making a determination. Their assessment will be made with respect to the outcomes of data protection in a third country, instead of being prescriptive about the form and means of protection, recognising that no two data protection regimes are identical.

The article also sets out a more concise and streamlined list of key factors that the Secretary of State must consider as part of their assessment. However, article 45B(2) is a non-exhaustive list, and the Secretary of State may also need to consider other matters in order to determine whether the required standard of protection exists.

Article 45C amends the system for formally reviewing data bridge regulations, removing the requirement for them to be reviewed periodically. The Secretary of State will still be subject to the requirement to monitor developments in other countries on an ongoing basis. Schedule 5 also amends article 46, which sets out the rules for controllers and processors to make international transfers of personal data using alternative transfer mechanisms.

The new article 46 requirements are tailored for data exporters to transfer defined types of data in specific circumstances. They stipulate that the data exporter, acting reasonably and proportionately, must consider that the standard of protection provided for the data subject would be "not materially lower" than the standard of protection in the UK in the specific circumstances of the transfer. The new requirements accommodate disparities between data exporters, where what is right for a multinational organisation transferring lots of sensitive data may not be right for a small charity making ad hoc transfers.

Schedule 5 also introduces article 47A, which provides a power for the Secretary of State to create or recognise new UK and non-UK alternative transfer mechanisms. The new power will help to future-proof the UK's international transfers regime by allowing the Government to shape international developments and react quickly to global trends, helping UK businesses connect and trade with their partners around the world.

Schedule 6 amends relevant parts of the Data Protection Act 2018 governing international transfers of personal data, which are governed by the law enforcement processing regime. Paragraph 4 omits the section governing transfers based on adequacy assessments and inserts a new provision to mirror the approach being adopted in schedule 5. As with the changes described in schedule 5, schedule 6

[Sir John Whittingdale]

amends the power in new section 74AA for the Secretary of State to make regulations approving transfers of personal data to another jurisdiction. It replaces the current list of considerations with a broader, non-exhaustive one. The schedule also clarifies the test found in new section 74AB that must be applied when regulations are made, giving greater clarity to the UK regulations decision-making process.

4 pm

Paragraph 6 amends the wording that provides for transfers outside the UK subject to "appropriate safeguards". To improve the effectiveness of transferring data internationally, the amended wording introduces the principles of reasonableness and proportionality to manage what can be reasonably expected of an organisation transferring the data. Further amendments clarify the rules for law enforcement transfers in the absence of regulations or appropriate safeguards. That route will still be permitted only when there are special circumstances that warrant the transfer, such as to prevent an immediate, serious threat to public security.

Schedule 6 further amends the section of the Data Protection Act that currently obliges UK data controllers to ensure that international partners seek consent from the UK in all cases before they share personal data with another country or international organisation. The reform will allow a UK controller to permit international parties to transfer personal data without the consent of the UK controller where they conclude that that is necessary to prevent an immediate, serious threat to public security or national security. The proposal would remove any delay to addressing serious and immediate threats.

Clause 21 introduces schedules 5 and 6, which reform the UK's international personal data transfers regime. The clause also introduces schedule 7, which contains consequential and transitional provisions supporting the amendments to the UK's regime for international transfer of data.

I come to amendment 104, which the Opposition have tabled. Should I deal with that now or allow the Opposition to speak to the amendment first, Mr Hollobone?

The Chair: The Minister is being very courteous and generous, and he makes a very sensible suggestion. Will he respond to amendment 104 after the Opposition have spoken to it?

Sir John Whittingdale: It would make sense to explain the reasons why we are not convinced after we have heard the arguments in favour.

The Chair: I call Stephanie Peacock.

Stephanie Peacock: I am grateful to the Minister, and I will focus my remarks particularly on the contents of schedule 5 before explaining the thought process behind amendment 104.

In the globalised world in which we live, we have an obligation to be outward looking and to consider not just the activities that take place in the UK, but those that occur worldwide. When it comes to data protection, that means accepting that data will likely need to travel across borders, and inserting appropriate safeguards so that UK citizens do not lose the protection of data protection laws if their personal data is transferred away from this country. The standard of those safeguards is absolutely crucial to the integrity of our entire data protection regime. After all, if a controller can simply send the personal data of UK citizens to a country that has limited data protection laws for processing that would be unlawful here, and if they can transfer that data back afterwards, in reality our laws are only as strong as the country with the weakest protections in the world.

As things stand, there is only a limited set of circumstances under which personal data can be transferred to a third party outside the UK. One such circumstance is where there is an adequacy agreement, similar to that which we have with the EU. For such an agreement to be reached, the Secretary of State must have considered many things, including the receiver's respect for human rights and data rules; the presence, or lack thereof, of a regulator, and its independence; and any international commitments they have made in relation to data protection. These amendments ensure that data can flow freely between the UK and another country as long as the level of protection received by citizens is not undermined by the regulatory structure in that country.

The Bill amends the adequacy-based framework and replaces it with a new outcomes-based approach through the data protection test. The test is met if the standard of the protection provided for data subjects, with regard to the general processing of personal data in the country or by the organisation, is not materially lower than the standard of protection under the UK GDPR and relevant parts of the DPA 2018.

When deciding whether the test is met, the Secretary of State must still consider many of the same things: their respect for human rights, the existence of a regulator, and international obligations. However, stakeholders such as Reset.tech and the TUC have expressed concern that the new test could mean that UK data is transferred to countries with lower standards of protection than previously. That is significant not just for data subjects in the UK, who may be faced with weaker rights, but for business, which fears that this may signify a divergence from the EU GDPR that could threaten the UK's own adequacy status. Losing this agreement would have real-world consequences for UK consumers and businesses to the tune of hundreds of millions of pounds. What conversations has the Minister had with representatives of the European Commission to ensure that the new data protection test does not threaten adequacy? Does he expect the new data protection test to result in the data of UK citizens being passed to countries with weaker standards than are allowed under the current regime?

Moving on to amendment 104, one reason why some stakeholders are expressing concern about the new rules is because they appear to omit article 44. As it stands, for those who are concerned about the level of data protection available to them as a result of international transfers, article 44 of the UK GDPR provides a guarantee that the integrity of the UK's data protection laws will be protected. Indeed, it sets out that all provisions relating to the international transfer of UK personal data

"shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

If UK data will not be transferred to countries with weaker protections, it is not clear why this simple guarantee would be removed. The amendment would clear up any confusion around that and reinsert the article so that data subjects can be reassured of the strength of this new data protection test and of their rights.

Again, it is important to emphasise that getting the clause right is absolutely essential, as it underpins the entire data protection regime in the country. Getting it wrong could cost a huge amount, rendering the Bill, the UK GDPR and the Data Protection Act 2018 essentially useless. It is likely that the Government do not intend to undermine their own regulatory framework. Reinserting the article would confirm that in the Bill, offering complete clarity that the new data protection test will not result in lower levels of protection for UK data subjects.

Sir John Whittingdale: We completely agree with the hon. Lady that we would not wish to see data transferred to countries that have an inferior data protection regime. However, we do not think amendment 104 is required to achieve that, because the reforms in chapter 5 already provide for a clear and high standard of protection when transferring personal data overseas. It states that the standard of protection in that country must not be "materially lower" than the standard under the UK GDPR. That ensures that high standards of data protection are maintained. In addition, we feel that the amendment would return us to the confusion of the existing regime. At present, the legislative framework makes it difficult for organisations and others to understand what standard needs to be applied when transferring personal data internationally, with several terms used in the chapter and in case law. Our reforms ensure that a clear standard applies, which maintains protection for personal data.

The hon. Lady raised the EU's data adequacy assessment. That is something that featured earlier in our debates on the Bill, and, as we heard from a number of our witnesses, including the information commissioner, there is no reason to believe that this in any way jeopardises the EU's assessment of the UK's data adequacy.

Government amendment 24 revises new article 45B(3)(c) of the UK GDPR, which is inserted by schedule 5 and which makes provision about the data protection test that must be satisfied for data bridge regulations to be made. An amendment to the Bill is required for the Secretary of State to retain the flexibility to make data bridge regulations covering transfers from the UK or elsewhere. The amendment will preserve the status quo under the current regime, in which the Secretary of State's power is not limited to covering only transfers from the UK. In addition to these amendments, four other minor and technical Government amendments —25, 26, 28 and 29—were tabled on 10 May.

Question put and agreed to.

Clause 21 accordingly ordered to stand part of the Bill.

Schedule 5

Transfers of personal data to third countries etc: general processing

Amendments made: 24, in schedule 5, page 147, line 3, leave out "from the United Kingdom" and insert

"to the country or organisation by means of processing to which this Regulation applies as described in Article 3".

New Article 45B(3)(c) of the UK GDPR explains how references to processing of personal data in a third country should be read (in the data protection test for regulations approving international transfers of personal data). This amendment changes a reference to data transferred from the United Kingdom to include certain data transferred from outside the United Kingdom.

Amendment 25, in schedule 5, page 147, line 12, leave out

"the transfer of personal data"

and insert "transfer".

This amendment and Amendment 26 simplify the wording in new Article 45B(4)(b) of the UK GDPR.

Amendment 26, in schedule 5, page 147, line 14, leave out

"the transfer of personal data"

and insert "transfer".—*(Sir John Whittingdale.)*

See the explanatory statement for Amendment 25.

Schedule 5, as amended, agreed to.

Schedule 6

Transfers of personal data to third countries etc: law enforcement processing

Amendments made: 27, in schedule 6, page 155, line 39, leave out "from the United Kingdom" and insert—

"to the country or organisation by means of processing to which this Act applies as described in section 207(2)".

New section 74AB(3)(c) of the Data Protection Act 2018 explains how references to processing of personal data in a third country should be read (in the data protection test for regulations approving international transfers of personal data). This amendment changes a reference to data transferred from the United Kingdom to include certain data transferred from outside the United Kingdom.

Amendment 28, in schedule 6, page 156, line 6, leave out

"the transfer of personal data"

and insert "transfer".

This amendment and Amendment 29 simplify the wording in new section 74AB(4)(b) of the Data Protection Act 2018.

Amendment 29, in schedule 6, page 156, line 8, leave out

"the transfer of personal data"

and insert "transfer".—*(Sir John Whittingdale.)*

See the explanatory statement for Amendment 28.

Schedule 6, as amended, agreed to.

Schedule 7 agreed to.

Clause 22

Safeguards for processing for research etc purposes

Sir John Whittingdale: I beg to move amendment 34, in clause 22, page 36, leave out lines 20 to 22.

This amendment and Amendment 37 transpose the requirement for processing of personal data for research, archiving and statistical purposes to be carried out subject to appropriate safeguards from the beginning to the end of new Article 84B of the UK GDPR.

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

Government amendments 35 to 39.

Clause stand part.

Clause 23 stand part.

Sir John Whittingdale: Clause 22 creates a new chapter in the UK GDPR that provides safeguards for the processing of personal data for the purposes of scientific research or historical research, archiving in the public

[Sir John Whittingdale]

interest, and for statistical purposes. Currently, the provisions that provide safeguards for those purposes are spread across the UK GDPR and the Data Protection Act 2018.

Clause 22 consolidates those safeguards in a new chapter 8A of the UK GDPR. Those safeguards ensure that the processing of personal data for research, archiving and statistical purposes does not cause substantial damage or substantial distress and that appropriate technical and organisational measures are in place to respect data minimisation. Clause 23 sets out consequential changes to the UK GDPR and Data Protection Act 2018 required as a result of the changes being made in clause 22 to consolidate safeguards for research.

Government amendments 34 to 39 are minor, technical amendments clarifying that, as part of the pre-existing additional requirement when processing for research, archiving and statistical purposes, a controller is to use anonymous—rather that personal—data, unless that means that those purposes cannot be fulfilled. It makes clear that processing to anonymise the personal data is permitted. On that basis, I commend the clauses, and indeed the Government amendments, to the Committee.

Stephanie Peacock: With regards to clause 22, it is pleasing to see a clause confirming the safeguards that are applicable when processing under the new research and scientific purposes. For example, it is welcome that it is set out that such processing must not cause substantial damage or distress to a data subject, must respect the principle of data minimisation and must not make decisions related to a particular data subject unless it is for approved medical research.

Those safeguards are especially important given the concerns that I laid out over the definition of scientific research in clause 2, which could lead to the abuse of data under the guise of legitimate research. I have no further comments on the clause or the Government's amendments to it at this stage, other than to reiterate that the definition of scientific research must have clear boundaries if any of the clauses that concern research are to be used as intended.

Clause 23 makes changes consequential on those in clause 22, so I refer to the substance of my remarks during the discussion of the previous clause.

Amendment 34 agreed to.

4.15 pm

Amendments made: 35, in clause 22, page 36, leave out lines 23 to 30 and insert—

"3A Personal data may only be processed for RAS purposes if—

(a) the processing consists of the collection of the personal data (whether from the data subject or otherwise),

(b) the processing is carried out in order to convert the personal data into information which can be processed in a manner which does not permit the identification of a living individual, or

(c) without the processing, the RAS purposes cannot be fulfilled."

This amendment replaces and clarifies the restriction in new Article 84B(2) and (3) of the UK GDPR on processing of personal data for research, archiving or statistical purposes. It makes clear that processing carried out for the purpose of anonymising personal data is permitted.

Amendment 36, in clause 22, page 36, line 31, leave out "2" and insert "3A".

This amendment is consequential on Amendment 35.

Amendment 37, in clause 22, page 36, line 34, at end insert—

"5. Processing of personal data for RAS purposes must be carried out subject to appropriate safeguards for the rights and freedoms of the data subject."

See the explanatory statement for Amendment 34.

Amendment 38, in clause 22, page 37, line 4, leave out "84B(1)" and insert "84B(5)".

This amendment is consequential on Amendments 34 and 37.

Amendment 39, in clause 22, page 38, line 14, leave out "84B(1)" and insert "84B(5)".—*(Sir John Whittingdale.)*

This amendment is consequential on Amendments 34 and 37.

Clause 22, as amended, ordered to stand part of the Bill.

Clause 23 ordered to stand part of the Bill.

Clause 24

National security exemption

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

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

Amendment 105, in clause 25, page 44, line 6, leave out "must consult the Commissioner" and insert

"must apply to the Commissioner for authorisation of the designation notice on the grounds that it satisfies subsection (1)(b)."

This amendment seeks to increase independent oversight of designation notices by replacing the requirement to consult the Commissioner with a requirement to seek the approval of the Commissioner.

Clauses 25 and 26 stand part.

Sir John Whittingdale: Clause 24 introduces an exemption that can be applied to the processing of personal data for law enforcement purposes under the law enforcement regime for the purposes of safeguarding national security. It will replace the current, more limited national security exemptions that exist in the law enforcement regime and mirror the existing exemptions in the UK GDPR and intelligence services regime.

The clause will allow organisations to exempt themselves from specified provisions in the law enforcement regime of the Data Protection Act 2018, such as some of the data protection principles and the rights of the individual, but only where it is necessary to do so for the purposes of safeguarding national security. Like the other exemptions in the Act, it must be applied on a case-by-case basis. There are limits to what the exemption applies to. The processing of data by law enforcement authorities must always be lawful, and the protections surrounding sensitive processing remain.

Subsection (2) amends the general processing regime of the Data Protection Act, regarding processing under UK GDPR, to remove the ability of organisations to exempt themselves, on the grounds of safeguarding national security, from article 77 of the UK GDPR, which provides the right for individuals to lodge a complaint with the Information Commissioner. That is because we do not consider exemption from that provision

necessary. The change will align the national security exemption applicable to UK GDPR processing with the other national security exemptions in the Data Protection Act 2018, which do not permit the exemption to be applied in relation to an individual's right to complain to the Commissioner.

The ability of a Minister of the Crown to issue a certificate certifying the application of the exemption for the purposes of safeguarding national security, which previously existed, is retained; clause 24(8) simply updates that provision to reflect the new exemption. That change will assist closer working between organisations operating under the three distinct data protection regimes by providing greater confidence that data that, for example, may be of importance to a police investigation but also pertinent to a separate national security operation can be properly safeguarded by both organisations. I will allow the hon. Member for Barnsley East to speak to amendment 105, because I wish to respond to her.

Stephanie Peacock: I am grateful to the Minister. I want to speak today about a concern that has been raised about clauses 24, 25 and 26, so I will address them before speaking to amendment 105.

In essence, the clauses increase the opportunities for competent authorities to operate in darkness when it comes to personal data through both national security certificates and designation notices. Though it may of course be important in some cases to adjust data protection regulation in a minimal way to protect national security or facilitate working with the intelligence services, important too is the right to understand how any competent authority is processing our personal data—particularly given the growing mistrust around police culture.

To cite one stark example of why data transparency in law enforcement is important, after Sarah Everard was murdered, more than 30 police officers were reportedly investigated for unnecessarily looking up her personal data. First, that demonstrates that there is a temptation for officers to access personal data without due reason, perhaps particularly when it is related to a high-profile case. Secondly, however, it shows that transparency does hold people accountable. Indeed, thankfully, the individuals who were accused of accessing the data were swiftly investigated. That would not have been possible if that transparency had been restricted—for example, had there been a national security certificate or a designation notice in place.

The powers to apply for the certificates and notices that allow the police and law enforcement authorities exemptions from data protection, although sometimes needed, must be used extremely sparingly and must be proportionate to the need to protect national security. However, that proportionate approach does not appear to be guaranteed in the Bill, despite it being a requirement in human rights law.

In their oral and written evidence, representatives from Rights and Security International warned that clauses 24 to 26 could actually violate the UK's obligations under the Human Rights Act 1998 and the European convention on human rights. Everything that the UK does, including in the name of national security or intelligence services, must comply with human rights and the ECHR. That means that any time there is interference with the privacy of people in the UK—which is considered a fundamental right—for it to be lawful, the law in question must do only what is truly necessary for national security. That necessity standard is a high one, and it does not take into account whether a change might be more convenient for a competent authority.

Will the Minister clearly explain in what way the potential powers given to law enforcement under clauses 24 to 26, in both national security certificates and designation notices, would be strictly proportionate and necessary for national security, rather than simply making the operations of law enforcement easier and more convenient?

Primarily, the concern is for those whose data could be used in a way that fundamentally infringes on their privacy, but there are practical concerns too. Any clauses that contain suspected violations of human rights could set up the Government for lengthy legal battles, both in the UK and at the European Court of Human Rights, about their data protection and surveillance regimes. Furthermore, any harm to the UK's important relationships with the EU around data could threaten the adequacy agreement which, as we have all repeatedly heard, is vital to our economy.

It is vital, then, that Minister confirms that both national security certificates and designation notices will be used only where necessary, and exemptions will be allowed only where necessary. If that cannot be satisfied, we must oppose the clauses.

I will now focus on amendment 105. Where powers are available to provide exemptions to privacy protections on grounds of national security, it is important that they are protected from exploitation, and not unduly concentrated in any individual's hands without appropriate checks and balances. However, Rights and Security International warned that that was not taken into appropriate consideration in clause 25. Instead, the power to issue designation notices has been concentrated almost entirely in the hands of the Secretary of State, with no accountability measures built in.

Designation notices allow for joint processing between a qualifying competent authority and the intelligence services, which could have greatly beneficial consequences for tackling crime and threats to our national security, but they will also allow for both those parties to be exempt from what are usually crucial data protections. They must therefore be used sparingly, and only when necessary and proportionate.

As we have seen—and as I will argue countless times—we cannot rely on the Secretary of State's acting in good faith. Our legislation must instead protect against a Secretary of State who acts in bad faith. Neither can we rely on the Secretary of State having the level of expertise needed to make complex and technical decisions, especially those that impact on national security and data rights at the same time.

Despite that, under clause 25(2), the Secretary of State alone can specify which competent authorities qualify as able to apply for a designation notice. Under subsection (3), it is the Secretary of state alone to whom qualifying competent authorities will jointly apply. It is the Secretary of State who reviews a notice and has the power to withdraw it, and it is the Secretary of State who makes transition arrangements.

Although there is a requirement in the Bill to consult the commissioner, the amendment seeks to formalise some independent oversight of the designation process

[Stephanie Peacock]

by ensuring that the commissioner has an actual say in approving the notices and adjusting the concentration of power so that it does not lie solely in the Secretary of State's hands. That would mean that should the Secretary of State act in bad faith, or lack the expertise needed to make such a decision—whether aware or unaware of this fact—the commissioner would be able to help to ensure that an informed and proportionate decision was made with regard to each notice applied for. This would not present any designation notices from being issued when they were genuinely necessary; it would simply safeguard their approval when they were.

Sir John Whittingdale: I assure the hon. Lady that clauses 25 and 26 are necessary for the improvement of national security. The reports on events such as the Manchester and Fishmongers' Hall terrorist incidents have demonstrated that better joined-up working between the intelligence services and law enforcement is in the public interest to safeguard national security. A current barrier to such effective joint working is that only the intelligence services can operate under part 4 of the Data Protection Act, which is drafted to reflect the unique operational nature of their processing.

Carol Monaghan: Of course, the reports on incidents such as those at Fishmongers' Hall and the Manchester Arena pointed to a general lack of effective collaboration between security forces and the police. It was not data that was the issue; it was collaboration.

Sir John Whittingdale: I certainly accept that greater collaboration would have been beneficial as well, but there was a problem with data sharing and that is what the clause is designed to address.

As the hon. Member for Barnsley East will know, law enforcement currently operates under part 3 of the Data Protection Act when processing data for law enforcement purposes. That means that even when they work together, law enforcement and the intelligence services must each undertake separate assessments regarding the same joint-working processing.

The Chair: Order. I am making a habit of interrupting the Minister—I do apologise—but we have some news from the Whip.

Ordered, That the debate be now adjourned.—*(Steve Double.)*

4.27 pm

Adjourned till Thursday 18 May at half-past Eleven o'clock.

Written evidence reported to the House

DPDIB10 John McVeigh, Principal Consultant, AssureMore

DPDIB11 Tim Bell, Managing Director, Data Protection Representative (UK) Limited (trading as DataRep UK)

DPDIB12 The Advertising Association.

DPDIB13 DPN Associates

DPDIB14 Shoosmiths LLP

DPDIB15 5Rights Foundation

DPDIB16 UK Competitive Telecommunications Association (UKCTA)

DPDIB17 Internet Services Providers' Association

DPDIB18 Judith Ratcliffe, Privacy Professional (further submission)

DPDIB19 Gener8

DPDIB20 Which?

DPDIB21 National AIDS Trust

DPDIB22 Sky

DPDIB23 Market Research Society (MRS)

DPDIB24 Lucy Purdon, Senior Tech Policy Fellow, Mozilla Foundation

DPDIB25 Hyperoptic

DPDIB26 UK Finance (supplementary submission)

DPDIB27 Medtronic plc (supplementary submission)

DPDIB28 Biometrics and Surveillance Camera Commissioner

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Fifth Sitting

Thursday 18 May 2023

(Morning)

CONTENTS

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 22 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
† Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Eastwood, Mark *(Dewsbury)* (Con)
† Henry, Darren *(Broxtowe)* (Con)
† Hunt, Jane *(Loughborough)* (Con)
† Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Monaghan, Carol *(Glasgow North West)* (SNP)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
Richards, Nicola *(West Bromwich East)* (Con)
† Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Public Bill Committee

Thursday 18 May 2023

(Morning)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

Clause 24

National security exemption

11.30 am

Question (16 May) again proposed, That the clause stand part of the Bill.

The Chair: I remind the Committee that with this we are discussing the following:

Amendment 105, in clause 25, page 44, line 6, leave out "must consult the Commissioner" and insert

"must apply to the Commissioner for authorisation of the designation notice on the grounds that it satisfies subsection (1)(b)."

This amendment seeks to increase independent oversight of designation notices by replacing the requirement to consult the Commissioner with a requirement to seek the approval of the Commissioner.

Clauses 25 and 26 stand part.

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): When the Committee last adjourned, I had already spoken to clauses 24 to 26 and was responding to amendment 105, which was tabled by the hon. Member for Barnsley East. However, let me give a quick recap.

Clauses 24 to 26 are essentially designed to enable better joined-up working between the intelligence services and law enforcement. To that end, they will allow qualifying authorities to use part 4 of the data protection regime, but the Secretary of State will be required to issue a designation notice. We believe that enabling qualifying competent authorities to jointly process data under one regime in authorised, specific circumstances will allow better control over data in a way that is not possible under two different data protection regimes.

Amendment 105 seeks to increase the role of the Information Commissioner's Office by requiring it to judge whether the designation notice is required for the purposes of safeguarding national security. The Bill requires the Secretary of State to consult the ICO as part of the Secretary of State's decision whether to grant a notice, but it is not the function of the ICO in its capacity as a regulator to assess national security requirements. The ICO's expertise is in data protection, not in national security, and it would be inappropriate for it to decide on the latter; that decision should be reserved to the Secretary of State. We believe that clause 25 provides significant safeguards through proposed new sections 82B and 82E, which provide respectively for legal challenge and annual review of a notice. In addition, should the notice no longer be required, the Secretary of State can withdraw it. For that reason, we cannot accept the amendment.

Stephanie Peacock (Barnsley East) (Lab): I spoke to amendment 105 in our last sitting. In summary, the Bill contains a requirement to consult the commissioner. The amendment seeks to formalise some of the independent oversight of the designation notice process so that the power does not lie solely in the Secretary of State's hands. The matter of the Secretary of State's power is obviously something with which we take issue throughout the Bill. The amendment would not stop any designation notice being issued where it is genuinely necessary; it would simply add a safeguard for its approval where it is not. For that reason, I will press the amendment to a vote.

Question put and agreed to.

Clause 24 accordingly ordered to stand part of the Bill.

Clause 25

Joint processing by intelligence services and competent authorities

Amendment proposed: 105, in clause 25, page 44, line 6, leave out "must consult the Commissioner" and insert "must apply to the Commissioner for authorisation of the designation notice on the grounds that it satisfies subsection (1)(b)."—*(Stephanie Peacock.)*

This amendment seeks to increase independent oversight of designation notices by replacing the requirement to consult the Commissioner with a requirement to seek the approval of the Commissioner.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 20]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Simmonds, David
Double, Steve	Whittingdale, rh Sir John
Eastwood, Mark	

Question accordingly negatived.

Clause 25 ordered to stand part of the Bill.

Clause 26 ordered to stand part of the Bill.

Clause 27

Duties of the Commissioner in carrying out functions

Amendment proposed: 106, in clause 27, page 47, line 27, after "subjects", insert "decision subjects,".—*(Stephanie Peacock.)*

This amendment would require the ICO to have regard to decision subjects (see NC12) as well as data subjects as part of its obligations.

The Committee divided: Ayes 6, Noes 9.

Division No. 21]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Simmonds, David
Double, Steve	Whittingdale, rh Sir John
Eastwood, Mark	

Question accordingly negatived.

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

Sir John Whittingdale: We now come to the provisions in the Bill relating to the powers of the Information Commissioner. Clause 27 will introduce a new strategic framework for the Information Commissioner when carrying out his functions under data protection legislation. The framework contains a principal data protection objective and a number of general duties.

The legislation does not currently provide the commissioner with a framework of strategic objectives to help to prioritise activities and resources, evaluate performance and be held accountable by stakeholders. Instead, the commissioner is obliged to fulfil a long list of tasks and functions without a clear strategic framework to guide his work.

The clause introduces a principal objective for the commissioner, first to secure an appropriate level of protection for personal data, taking into account the interests of data subjects, controllers and others along with matters of general public interest, and secondly to promote public trust and confidence in the processing of personal data. This principal objective will replace section 2(2) of the Data Protection Act 2018.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): How does the Minister think the words

"an appropriate level of protection for personal data"

should be understood by the Information Commissioner? Is it in the light of the duties that follow, or what?

Sir John Whittingdale: Obviously that is a matter for the Information Commissioner, but that is the overriding principal objective. I am about to set out some of the other objectives that the clause will introduce, but it is made very clear that the principal objective is to ensure the appropriate level of protection. Precisely how the Information Commissioner interprets "appropriate level of protection" is a matter for him, but I think it is fairly clear what that should entail, as he himself set out in his evidence.

As I have said, clause 27 introduces new duties that the commissioner must consider where they are relevant to his work in carrying out data protection functions: the desirability of promoting innovation and competition; the importance of the prevention, investigation, detection and prosecution of criminal offences; the need to safeguard public security and national security; and, where necessary, the need to consult other regulators when considering how the ICO's work may affect economic growth, innovation and competition. There is also the statement of strategic priorities, which is introduced by clause 28. However, as I have indicated to the hon. Member for Newcastle upon Tyne Central, the commissioner will be clear that his primary focus should be to achieve the principal objective.

Clause 27 also introduces new reporting requirements for the commissioner in relation to the strategic framework. The commissioner will be required to publish a forward-looking strategy outlining how he intends to meet the new principal objective and duties, as well as pre-existing duties in the Deregulation Act 2015 and the Legislative and Regulatory Reform Act 2006.

Finally, the commissioner will be required to publish a review of what he has done to comply with the principal objective, and with the new and existing duties, in his annual report.

Carol Monaghan (Glasgow North West) (SNP): I wonder whether part of the strategy might include a list of fees that could potentially be charged for accessing data. This idea of fees seems to be quite vague in terms of amounts and levels, so it would be useful to have some more information on that.

Sir John Whittingdale: I think we will come on to some of the questions around the fees that are potentially payable, particularly by those organisations that may be required to provide more evidence, and the costs that that could entail. I will return to that subject shortly.

The new strategic framework acknowledges the breadth of the ICO's remit and its impact on other areas. We believe that it will provide clarity for the commissioner, businesses and the general public on the commissioner's objectives and duties. I therefore commend clause 27 to the Committee.

Stephanie Peacock: The importance to any data protection regime of an independent, well-functioning regulator cannot be overstated. The ICO, which is soon to be the Information Commission as a result of this Bill, is no exception to that rule. It is a crucial piece of the puzzle in our regime to uphold the information rights set out in regulation. Importantly, it works in the interests of the general public. The significance of an independent regulator is also recognised by the European Commission, which deems it essential to any adequacy agreement. The general duties of our regulator, such as those set out in this clause, are therefore vital because they form the foundations on which it operates and the principles to which it must be accountable.

Although the duties are more an indicator of overarching direction than a prescriptive list of duties, they should still aim to reflect the wide range of tasks that the regulator carries out and the values with which they do so. On the whole, the clause does this well. Indeed, the principal objective for the commissioner set out in this clause, which is

"to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest, and…to promote public trust and confidence in the processing of personal data"

is a good overarching starting point. It simply outlines the basic functions of the regulator that we should all be able to get behind, even if the Bill itself does disappointingly little to encourage the promotion of public trust in data processing.

It is particularly welcome that the principal objective includes specific regard to

"matters of general public interest."

This should cover things like the need to consider sustainability and societal impact. However, it is a shame that that is not made explicit among the sub-objectives,

[Stephanie Peacock]

which require the commissioner to have regard to the likes of promoting innovation and safeguarding national security. That would have ingrained in our culture a desire to unlock data for the wider good, not just for the benefit of big tech. Overall, however, the responsibilities set out in the clause, and the need to report on fulfilling them, seem to reflect the task and value of the regulator fairly and accurately.

Sir John Whittingdale: I think that was slightly qualified support for the clause. Nevertheless, we welcome the support of the Opposition.

Question put and agreed to.

Clause 27 accordingly ordered to stand part of the Bill.

Clause 28

STRATEGIC PRIORITIES

11.45 am

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

Sir John Whittingdale: Clause 28 provides a power for the Secretary of State to prepare a statement of strategic priorities relating to data protection as part of the new strategic framework for the Information Commissioner. The statement will contain only the Government's data protection priorities, and the Secretary of State may choose to include both domestic and international priorities. That will enable the Government to provide a transparent statement of how their data protection priorities fit in with their wider agenda, giving the commissioner, we hope, helpful context.

Although the commissioner must take the statement into account when carrying out his functions, he is not required to act in accordance with it. That means that the statement will not be used in a way to direct what the commissioner may and may not do. Once the statement is drafted, the Secretary of State will be required to lay it before Parliament, where it will be subject to the negative resolution procedure before it can be designated. The commissioner will need to consider the statement when carrying out functions under the data protection legislation, except functions relating to a particular person, case or investigation.

Once designated, the commissioner will be required to respond to the statement, outlining how he intends to consider it in future data protection work. The commissioner will also be required to report on how he has considered the statement in his annual report. I commend the clause to the Committee.

Stephanie Peacock: Clause 28 requires that every three years the Secretary of State publish a statement of strategic priorities for the commissioner to consider, respond to, and have regard to. The statement would be subject to the negative resolution procedure in Parliament, and the commissioner would be obliged to report on what they have done to comply with it annually. Taken in good faith, I see what the clause was intended to achieve. It is, of course, important that the Government's data priorities are understood by the commissioner. It is also vital that we ensure that the regulator functions in line with the most relevant issues of the day, given the rapidly evolving landscape of technology.

A statement of strategic priorities could, in theory, allow the Government to set out their priorities on data policy in a transparent way, allowing both Ministers and the ICO to be held accountable for their relationship. However, there is and must be a line drawn between the ICO understanding the modern regulatory regime that it will be expected to uphold and political interference in the activities and priorities of the ICO. The Open Rights Group, among others, has expressed concern that the introduction of a statement of strategic priorities could cross that line, exposing the ICO to political direction, making it subject to culture wars and leaving it vulnerable to corporate capture or even corruption.

Although the degree to which those consequences would become a reality given the current strength of our regulator might be up for debate, the very concept of the Government setting out a statement of strategic priorities that must be adhered to by the commissioner at the very least sets out a need for the ICO to follow some sort of politically led direction, something that seems counterintuitive with respect to independence. As I have already argued, an independent ICO is vital not only directly, for data subjects to be sure that their rights will be implemented and for controllers to be sure of their obligations, but indirectly, as a crucial component of our EU adequacy agreement.

Even though the clause may not be intended to threaten independence, we must be extremely careful not to unintentionally embark on a slippery slope, particularly as there are other mechanisms for ensuring that the ICO keeps up with the times and has a transparent relationship with Government. In 2022, the ICO published its new strategic plan, ICO25, which sets out why its work is important, what it wants to be known for and by whom, and how it intends to achieve that by 2025. It describes the ICO's purpose, objectives and values and the shift in approach that it aims to achieve through the life of the plan, acknowledging that its work is

"complex, fast moving and ever changing."

The plan was informed by extensive stakeholder consultation and by the responsibilities that the ICO has been given by Parliament. There are therefore ways for the ICO to communicate openly with Government, Parliament and other relevant stakeholders to ensure that its direction is in keeping with the most relevant challenges and with updates to legislation and Government activity. Ministers might have been better off encouraging transparent reviews, consultations and strategies of that kind, rather than prompting any sort of interference from politicians with the ICO's priorities.

Sir John Whittingdale: We agree about the importance of the independence of the Information Commissioner, but I do not think that the statement, as we have set out, is an attempt to interfere with that. I remind the hon. Lady that in relation to the statement of strategic priorities, she asked the Information Commissioner himself:

"Do you perceive that having any impact on your organisation's ability to act independently of political direction?",

and he replied:

"No, I do not believe it will undermine our independence at all."—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 6, Q3.]

Stephanie Peacock: The Minister is right to quote the evidence session, but he will perhaps also remember that in a later session Ms Irvine from the Law Society of Scotland said that she was surprised by the answer given by the Information Commissioner.

Sir John Whittingdale: Ms Irvine may have been surprised. I have to say that we were not. What the Information Commissioner said absolutely chimed with our view of the statement, so I am afraid on this occasion I will disagree with the Law Society of Scotland.

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

The Committee divided: Ayes 9, Noes 6.

Division No. 22]

AYES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Simmonds, David
Double, Steve	Whittingdale, rh Sir John
Eastwood, Mark	

NOES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

Question accordingly agreed to.

Clause 28 ordered to stand part of the Bill.

Clause 29

CODES OF PRACTICE FOR THE PROCESSING OF PERSONAL DATA

Amendment proposed: 108, in clause 29, page 53, line 11, at end insert—"(ba) decision subjects;".—*(Stephanie Peacock.)*

This amendment, together with Amendments 109 and 110, would require codes of conduct produced by the ICO to have regard to decision subjects (see NC12) as well as data subjects.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 23]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Simmonds, David
Double, Steve	Whittingdale, rh Sir John
Eastwood, Mark	

Question accordingly negatived.

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

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

Clause 30 stand part.

Amendment 111, in clause 31, page 56, line 30, leave out lines 30 and 31 and insert—

"(6) If the Commissioner submits a revised code under subsection (5)(b), the Secretary of State must approve the code."

This amendment seeks to limit the ability of the Secretary of State to require the Commissioner to provide a revised code to only one occasion, after which the Secretary of State must approve the revised code.

Clause 31 stand part.

Sir John Whittingdale: Given the significant number of ways in which personal data can be used, we believe that it is important that the regulator provides guidance for data controllers, particularly on complex and technical areas of the law, and that the guidance should be accessible and enable compliance with the legislation efficiently and easily. We are therefore making a number of reforms to the process by which the Information Commissioner produces statutory codes of practice.

Clause 29 is a technical measure that ensures that all statutory codes of practice issued under the Data Protection Act 2018 follow the same parliamentary procedures, have the same legal effect, and are published and kept under review by the Information Commissioner. Under sections 121 to 124 of the Data Protection Act, the commissioner is obliged to publish four statutory codes of practice: the data sharing code, the direct marketing code, the age-appropriate design code, and the data protection and journalism code. The DPA includes provisions concerning the parliamentary approval process, requirements for publication and review by the commissioner, and details of the legal effect of each of the codes. So far, the commissioner has completed the data sharing code and the age-appropriate design code.

Section 128 of the Act permits the Secretary of State to make regulations requiring the Information Commissioner to prepare other codes that give guidance as to good practice in the processing of personal data. Those powers have not yet been used, but may be useful in the future. However, due to the current drafting of the provisions, any codes required by regulations made by the Secretary of State and issued by the commissioner would not be subject to the same formal parliamentary approval process or review requirements as the codes issued under sections 121 to 124. In addition, they do not have the same legal effect, and courts and tribunals would not be required to take a relevant provision of the code into account when determining a relevant question. Clearly, it is not appropriate to have two different standards of statutory codes of practice. To address that, clause 29 replaces the original section 128 with new section 124A, so that codes required in regulations made by the Secretary of State follow a similar procedure to codes issued under sections 121 to 124.

New section 124A provides the Secretary of State with the power to make regulations requiring the commissioner to produce codes of practice giving guidance as to good practice in the processing of personal data. Before preparing any code, the commissioner must consult the Secretary of State and other interested parties such as trade associations, data subjects and groups representing data subjects. That is similar to the consultation requirements for the existing codes. The parliamentary approval processes and requirements for the ICO to keep existing codes under review are also extended to

[Sir John Whittingdale]

any new codes required by the Secretary of State. The amendment also ensures that those codes requested by the Secretary of State have the same legal effect as those set out on the face of the DPA.

Clauses 30 and 31 introduce reforms to the process by which the commissioner develops statutory codes of practice for data protection. They require the commissioner to undertake and publish impact assessments, consult with a panel of experts during the development of a code, and submit the final version of a code to the Secretary of State for approval. Those processes will apply to the four statutory codes that the commissioner is already required to produce and to any new statutory codes on the processing of personal data that the commissioner is required to prepare under regulation made by the Secretary of State.

The commissioner will be required to set up and consult a panel of experts when drafting a statutory code. That panel will be made up of relevant stakeholders and, although the commissioner will have discretion over its membership, he or she will be required to explain how the panel was chosen. The panel will consider a draft of a statutory code and submit a report of its recommendations to the commissioner. The commissioner will be required to publish the panel's response to the code and, if he chooses not to follow a recommendation, the reasons must also be published.

Clause 30 also requires the commissioner to publish impact assessments setting out who will be affected by the new or amended code and the impact it will have on them. While the commissioner currently carries out impact assessments when developing codes of practice, we believe that there are advantages to formalising an approach on the face of the legislation to ensure consistency.

Given the importance of the statutory codes, we believe it is important that there is a further degree of democratic accountability within the process. Therefore, clause 31 requires the commissioner to submit the final version of a statutory code to the Secretary of State for approval.

On that basis, I commend the relevant clauses to the Committee, but I am aware that the hon. Member for Barnsley East wishes to propose an amendment.

Stephanie Peacock: I turn first to clauses 29 and 30. Codes of practice will become increasingly important as the remit of the ICO expands and modernises. As such, it is important that the codes are developed in a way that is conducive to the product being as effective and useful as possible.

Although the ICO already carries out impact assessments for new codes of practice, that is only done as best practice and currently does not have any statutory underpinning. It is therefore pleasing to see clauses that will require consistency and high standards when developing new codes, ensuring that the resulting products are as comprehensive and helpful as possible. It is welcome, for example, to see that experts will be consulted in the process of developing these codes, including Government officials, trade associations and data subjects. It is also good to see that the commissioner will be required to publish a statement relating to the establishment of the expert panel, including how and why members were selected.

12 noon

Given recent scandals that have shown that appointments to positions of power can be vulnerable, it is good practice to have transparency on the credentials of the panel, and how each of them came to be in such a position. That transparency is also reflected in the requirement for the commissioner to publish an explanation in any case where the panel's recommendations are not accepted. That will ensure that proper consideration must be taken of the panel's input, and it makes the commissioner accountable to the public.

I turn to clause 31 and amendment 111. Given the transparent and comprehensive statutory procedure set out in clause 30 to ensure that codes of practice are developed in conjunction with officials, industry and data subjects, and informed by expertise, the addition of the clause seems somewhat counterintuitive. Indeed, having already passed through the rigorous and transparent procedure, the clause allows codes of practice to be subject to endless interference from the Secretary of State, who—no matter their level of expertise or their intention—would be able to veto the codes, and send them back to the commissioner with recommendations for changes as many times as they wanted or needed to.

That level of interference from a politically appointed and motivated Minister in the product of an independent regulator has caused a lot of concern across a range of stakeholders. Indeed, almost every civil society group and trade association I engaged with in the run up to the Committee has raised concerns that the procedure could threaten the independence of the ICO altogether. That was also reflected in the consultation responses to the proposal in "Data: a new direction," in which the Government admitted that a majority of people disagreed, citing concerns about the risk to independence.

This matters—not just inherently, but for public trust in the entire system of data protection. Any interpretation or potential that the independence of the commissioner is being downgraded could have a knock-on impact on the public's ability to trust in its functions and, in turn, their ability to exercise their rights. Furthermore, it matters for the maintenance of our adequacy agreement with the EU, as such agreements rely heavily on the existence of a truly independent and functioning regulator.

I will again cite the figures from the Government's own impact assessment, in which it is acknowledged that losing the agreement could cost up to £460 million as a one-off and £410 million every year afterwards. That is based on a direct reduction in UK-EU trade, and it may be even larger when accounting for onward supply chains with trade with third countries. It is therefore a concern for not just those most interested in data rights—though their input is, of course, crucial—but every single business that relies on EU adequacy and all of us who live in the economy that benefits from it.

To try to counteract concerns over the process, the Secretary of State will be required to publish their rationale for approving or not approving a code. Though the principle of transparency is always welcome, it is unfortunately not enough in this instance to justify any compromise—perceived or otherwise—to the independence of the ICO. Furthermore, there are no stated limits on the reasons that a Secretary of State might be able to refuse a code, even if they are made in bad faith or under severe misguidance, meaning that further harms may occur as a result of the changes. Given the scale of

the risks I have outlined, I am keen to hear from the Minister what the real benefit of the clause is. What value is there in the Secretary of State being able to endlessly interfere with an expertly formed code that they themselves have requested?

Amendment 111 recognises that there may be a very limited set of circumstances in which the Secretary of State may wish to comment on a code and correct an oversight or major misinterpretation of the law. Indeed, the Government say in their consultation response that the measure is intended as a "final safeguard". However, such instances should take only one round of amendments to resolve. The amendment would therefore accommodate one statement from the Secretary of State but give the regulator the ultimate say on its contents, ensuring that there is no risk of its independence being at stake. Anything more than that would put data rights, independence, and potentially adequacy at risk.

Sir John Whittingdale: I welcome the support of the Opposition for many of the principles contained in the clauses. I turn to amendment 111, tabled by the hon. Lady. As the clause originally sets out, once the commissioner is issued the final version of the code, the Secretary of State decides whether to approve it. If they do approve the code, it will be laid before Parliament for final approval. If they do not, they are required to publish their reasons.

The amendment would place a limit on that, so that the Secretary of State would be able to reject the final version of the code only once. If the code is revised by the commissioner in the light of the comments of the Secretary of State and resubmitted, under the amendment the Secretary of State would have to lay the code in Parliament for final approval. Although I understand the concern behind the amendment, we do not believe it to be justified. I understand that the hon. Lady does not want a code to be rejected multiple times, but we regard this as a final safeguard and it will be fully transparent. We are absolutely committed to maintaining the commissioner's independence, but we think it also important that the Government have the opportunity to give a view before the code is laid before Parliament and for Parliament to give final approval. The amendment would unduly limit the Government's ability to provide as necessary that further degree of democratic accountability.

The hon. Lady referred to the importance of maintaining adequacy, which we have already touched on. I fully share her view on its importance to the wider functioning of the economy, but when she raised the matter with the Information Commissioner he did not believe that it posed any risk. Indeed, he went on to point out:

"A failure of the Secretary of State to table and issue a proposed code would not affect the way in which the commissioner discharges his or her enforcement functions. We would still be able to investigate matters and find them in breach, regardless of whether that finding was consistent with the Secretary of State's view of the law."—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 6-7, Q4.]

On that basis, we think that there should be the ongoing ability for the Secretary of State—and, through the Secretary of State, Parliament—to approve the final version of the code, but we do not feel that this interferes with the Information Commissioner's ability to carry out his functions, nor does it represent any view as to our adequacy agreement.

Stephanie Peacock: The problem is that the Government are operating on the basis that everyone is acting in good faith, and although I am sure that the Minister and the current Secretary of State are doing so, we do not know what the future holds. It was incredibly encouraging that throughout the evidence sessions a number of witnesses said they did not feel that adequacy was at threat. That is welcome and reassuring, but only the EU Commission can give us adequacy. I am afraid the Minister simply has not done enough to alleviate my concerns about the independence of the ICO. I understand that the Minister disagrees with the Law Society of Scotland, but the full quote was:

"The ICO is tasked with producing statutory codes of conduct, which are incredibly useful for my clients and for anyone working in this sector. The fact that the Secretary of State can, in effect, overrule these is concerning, and it must be seen as a limit on the Information Commissioner's independence."—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 74, Q156.]

As such, I will push my amendment to a vote.

Question put and agreed to.

Clause 29 accordingly ordered to stand part of the Bill.

Clause 30 ordered to stand part of the Bill.

Clause 31

CODES OF PRACTICE: APPROVAL BY THE SECRETARY OF STATE

Amendment proposed: 111, in clause 31, page 56, line 30, leave out lines 30 and 31 and insert—

"(6) If the Commissioner submits a revised code under subsection (5)(b), the Secretary of State must approve the code."—*(Stephanie Peacock.)*

This amendment seeks to limit the ability of the Secretary of State to require the Commissioner to provide a revised code to only one occasion, after which the Secretary of State must approve the revised code.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 24]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Simmonds, David
Double, Steve	Whittingdale, rh Sir John
Eastwood, Mark	

Question accordingly negatived.

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

The Committee divided: Ayes 9, Noes 6.

Division No. 25]

AYES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Simmonds, David
Double, Steve	Whittingdale, rh Sir John
Eastwood, Mark	

NOES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

Question accordingly agreed to.

Clause 31 ordered to stand part of the Bill.

Clause 32

VEXATIOUS OR EXCESSIVE REQUESTS MADE TO THE COMMISSIONER

Amendments made: 40, in clause 32, page 57, line 16, leave out paragraphs (a) and (b) insert—

"(a) for the heading substitute "Vexatious or excessive requests",

(b) before subsection (1) insert—

"(A1) This section makes provision about cases in which a request made to the Commissioner, to which the Commissioner is required or authorised to respond under the data protection legislation, is vexatious or excessive (see section 204A).",

(ba) in subsection (1) omit the words from the beginning to "excessive,",

(bb) after subsection (1) insert—

"(1A) In subsection (1)—

(a) the reference in paragraph (a) to charging a reasonable fee is, in a case in which section 134 is relevant, a reference to doing so under that section, and

(b) paragraph (b) is not to be read as implying anything about whether the Commissioner may refuse to act on requests that are neither vexatious nor excessive.","

This amendment adds further amendments of section 135 of the Data Protection Act 2018 to clause 32 to make clear that the Information Commissioner may refuse to deal with a vexatious or excessive request made by any person.

Amendment 41, in clause 32, page 57, line 21, after "(3)" insert "—

"(i) for "(1)" substitute "(A1)", and

(ii)".—*(Sir John Whittingdale.)*

This amendment is consequential on Amendment 40.

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

Sir John Whittingdale: Taking advantage of your invitation, Mr Hollobone, I shall speak only briefly. The UK's data protection framework allows a data subject or data protection officer to make a request to the Information Commissioner for information concerning the exercise of their data protection rights. The commissioner is expected to respond to a data subject or data protection officer and make no charge in the majority of cases, but the commissioner can refuse to respond or charge a reasonable fee for a response to a request when it is "manifestly unfounded or excessive". Clause 7 changes the "manifestly unfounded or excessive" threshold for all requests from data subjects across the UK data protection framework to "vexatious or excessive". Clause 32 replicates that language, inserting the same new threshold into section 135 of the Data Protection Act 2018, to ensure that the Information Commissioner's exemption is consistent across the legislation. I urge the Committee to agree to the clause.

Stephanie Peacock: The new threshold contained in the clause has been discussed in debates under clause 7, and I refer hon. Members to my remarks in those debates, as many of the same concerns apply. The guidance that will be needed to interpret the terms "vexatious" and "excessive" should be no less applicable to the Information Commissioner, whose co-operation with data subjects and transparency should be exemplary, not least because the functioning of the regulator inherently sets an example for other organisations on how the rules should be followed.

Question put and agreed to.

Clause 32, as amended, accordingly ordered to stand part of the Bill.

Clause 33

ANALYSIS OF PERFORMANCE

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

Sir John Whittingdale: Clause 33 introduces the requirement for the Information Commissioner to prepare and publish an analysis of their performance, using key performance indicators. The regulator will be required to publish that analysis at least annually. The commissioner will have the discretion to decide which factors effectively measure their performance.

Improving the commissioner's monitoring and reporting mechanisms will strengthen their accountability to Parliament, organisations and the public, who have an interest in the commissioner's effectiveness. Performance measurement will also have benefits for the commissioner, including by supporting their work of measuring progress towards their objectives and ensuring that resources are prioritised in the right areas. I urge that clause 33 stand part of the Bill.

Stephanie Peacock: I welcome the clause, as did the majority of respondents who supported the proposal in the "Data: a new direction" consultation. As recognised by the Government's response to their consultation, respondents felt the proposal would allow for the performance of the ICO to be assessed publicly and provide evidence of how the ICO is meeting its statutory obligations. We should do all we can to promote accountability, transparency and public awareness of the obligations and performance of the ICO. The clause allows for just that.

Question put and agreed to.

Clause 33 accordingly ordered to stand part of the Bill.

Clause 34

POWER OF THE COMMISSIONER TO REQUIRE DOCUMENTS

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

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

Clauses 35 to 38 stand part.

Government amendment 47.

Clause 42 stand part.

12.15 pm

Sir John Whittingdale: This is a slightly chunkier set of clauses and amendments, so I will not be as brief as in the last two debates.

Clause 34 is a clarificatory amendment to the Information Commissioner's powers in section 142 of the Data Protection Act to require information. Its purpose is to clarify the commissioner's existing powers to put it beyond doubt that the commissioner can require specific documents as well as information when using the information notice power. Subsections (3) to (7) of the clause make consequential amendments to references to information notices elsewhere in the Data Protection Act.

Clause 35 makes provision for the Information Commissioner to require a data controller or processor to commission a report from an approved person on a specified matter when exercising the power under section 146 of the Data Protection Act to issue an assessment notice. The aim of the power is to ensure that the regulator can access information necessary to its investigations.

In the event of a data breach, the commissioner is heavily dependent on the information that the organisation provides. If it fails to share information—for example, because it lacks the capability to provide it—that can limit the commissioner's ability to conduct a thorough investigation. Of course, if the organisation is able to provide the necessary information, it is not expected that the power would be used. The commissioner is required to act proportionately, so we expect that the power would be used only in a small minority of investigations, likely to be those that are particularly complex and technical in nature.

Clause 36 grants the Information Commissioner the power to require a person to attend an interview and answer questions when investigating a suspected failure to comply with data protection legislation. At the moment, the Information Commissioner can only interview people who attend voluntarily, which means there is a heavy reliance on documentary evidence. Sometimes that is ambiguous or incomplete and can lead to uncertainty. The ability to require a person to attend an interview will help to explain an organisation's practices or evidence submitted, and circumvent a protracted and potentially fruitless series of back-and-forth communication via information notices. The power is based on existing comparable powers for the Financial Conduct Authority and the Competition and Markets Authority.

Clause 37 amends the provisions for the Information Commissioner to impose penalties set out in the Data Protection Act. It will allow the commissioner more time, where needed, to issue a final penalty notice after issuing a notice of intent. At the moment the Act requires the commissioner to issue a notice of intent to issue a penalty notice; the commissioner then has up to six months to issue the penalty notice unless an extension is agreed. That can prove difficult in some cases—for instance, if the organisation under investigation submits new evidence that affects the case at a late stage, or when the legal representations are particularly complex. The clause allows the regulator more time to issue a final penalty notice after issuing a notice of intent, where that is needed. That will benefit business, as it means the commissioner can give organisations more time to prepare their representations, and will result in better outcomes by ensuring that the commissioner has sufficient time to assess representations and draw his conclusions.

Clause 38 introduces the requirement for the Information Commissioner to produce and publish an annual report on regulatory activity. The report will include the commissioner's investigatory activity and how the regulator has exercised its enforcement powers. That will lead to greater transparency of the commissioner's regulatory activity.

Clauses 34 to 37, as I said, make changes to the Data Protection Act 2018 in respect of the Information Commissioner's enforcement powers. Consequential on clauses 35 and 36, clause 42 makes changes to the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016, known as the EITSET regulations. The EITSET regulations extend and modify the Information Commissioner's enforcement powers to apply to its role as the supervisory body for trust service providers under the UK regulations on electronic identification and trust services for electronic transactions, known as the UK eIDAS. Clause 42 amends the EITSET regulations to ensure that the new enforcement powers introduced by clauses 34 to 37 are available to the Information Commissioner for the purposes of regulating trust service providers.

The new powers will help to ensure that the Information Commissioner is able to access the evidence needed to inform investigations. The powers will result in more informed investigations and, we believe, better outcomes. Clause 42 ensures that the Information Commissioner will continue to be able to act as an effective supervisory body for trust service providers established in the UK.

Government amendment 47 amends schedule 2 to the EITSET regulations. The amendment 2 is consequential to the amendment of section 155(3)(c) of the Data Protection Act made by schedule 4 to the Bill. The amendment to schedule 2 will remove the reference to consultation under section 65 of the Data Protection Act when section 155 is applied. It is necessary to remove reference to section 65 of the Data Protection Act when section 155 is applied with modification under schedule 2, as consultation requirements under that section are not relevant to the regulation of trust service providers under the UK eIDAS.

I hope that that is helpful to Members in explaining the merits of our approach to ensuring that the Information Commissioner has the right enforcement tools at its disposal and continues to be an effective and transparent regulator. I commend the clauses and Government amendment 47 to the Committee.

Stephanie Peacock: I will speak to each of the relevant clauses in turn. On clause 34, I am satisfied that the clarification that the Information Commissioner can require documents as well as information is necessary and will be of use to the regulator. I am pleased therefore pleased to accept the clause as drafted and to move on to the other clauses in this part.

Clause 35 provides for the commissioner to require an approved person to prepare a report on a specified matter, as well as to provide statutory guidance on, first, the factors it considers when deciding to require such a report and, secondly, the factors it considers when determining whom the approved person might be. That

[Stephanie Peacock]

power to commission technical reports is one that the vast majority of respondents to the "Data: a new direction" consultation supported, as they felt it would lead to better informed ICO investigations. Any measures that help the ICO to carry out its duties rigorously and to better effect, while ensuring that relevant safeguards apply, are measures that I believe Members across the Committee will want to support.

In the consultation, however, the power was originally framed to commission a "technical report", implying that it would be limited to particularly complex and technical investigations where there is significant risk of harm or detriment to data subjects. Although the commissioner is required to produce guidance on the circumstances in which a report might be required, I would still like clarification from the Minister of why such a limit was not included in the Bill as drafted. Does he expect it to be covered by the guidance produced by the ICO? Such a clarification is necessary not because we are against clause 35 in principle, just in acknowledgement that ICO's powers—indeed, enforcement powers generally—must always be proportionate to the task at hand.

Furthermore, some stakeholders have said that it is unclear whether privilege will attach to reports required by the ICO and whether they may be disclosable to third parties who request copies of them. Greater clarity about how the power will operate in practice would therefore be appreciated.

Turning to clause 36, it is a core function of the ICO to monitor and enforce the UK's data protection legislation and rules, providing accountability against the activities of all controllers, processors and individuals. To fulfil that function, the ICO may have to conduct an investigation to establish a body of evidence and determine whether someone has failed to comply with the legislation. The Government's consultation document said that the ICO sometimes faces problems engaging organisations in those investigations, despite their having a duty to co-operate fully, especially in relation to interviews, as many people are nervous of negative consequences in their life or career if they participate in one. However, interviews are a crucial tool for investigations, as not all the relevant evidence will be available in written form. Indeed, that may become even more the case after the passing of this Bill, due to the reduced requirements to keep records, conduct data protection impact assessments and assign data protection officers—all of which contribute to a larger pool of documentation tracking data processing.

Clause 36, which will explicitly allow the ICO to compel witnesses to comply with interviews as part of an investigation, will, where necessary, ensure that as much relevant evidence as possible is obtained to inform the ICO's judgment. That is something that we absolutely welcome. It is also welcome to see the safeguards that will be put in place under this clause, including the right not to self-incriminate and exemptions from giving answers that would infringe legal professional privilege or parliamentary privilege. That will ensure that the investigatory powers of the ICO stay proportionate to the issues at hand. In short, clause 36 is one that I am happy to support. After all, what is the purpose of us ensuring that data protection legislation is fit for purpose here today if the ICO is unable to actually determine whether anyone is complying?

On clause 37, it seems entirely reasonable that the ICO may require more than the standard six months to issue a penalty notice in particularly complex investigations. Of course, it remains important that the operations of the ICO are not allowed to slow unduly in cases where a penalty can be issued in the usual timeframe, but where the subject matter is particularly complicated, it makes sense to allow the ICO an extension to enable the investigation to be concluded in the proper, typically comprehensive manner. Indeed, complex investigations may be more common as we adjust to the new data legislation and a rapidly evolving technological landscape. By conducting the investigations properly and paying due attention to particularly technical issues, new precedents can be set that will speed up the regulator's processes on the whole. Clause 37 is therefore welcomed by us, as it was by the majority of respondents to the Government's consultation.

Turning to clause 38, as we have said multiple times throughout the progress of this Bill and in Committee, transparency and data protection should go hand in hand. Requiring the ICO to publish information each year on the investigations it has undertaken and the powers it has used will embed a further level of transparency into the regulatory system. Transparency breeds accountability, and requiring the regulator to publish information on the powers it is using will encourage such powers to be used proportionately and appropriately. Publishing an annual report with that information should also give us a better idea of how effectively the new regulatory regime is working. For example, a high volume of cases on a recurring issue could indicate a problem within the framework that needs addressing. Overall, it is welcome that Parliament and the public should be privy to information about how the ICO is discharging its regulatory functions. As a result, I am pleased to support clause 38.

Finally, the amendments to clause 42 are of a consequential nature, and I am happy to proceed without asking any further questions about them.

Sir John Whittingdale: I am most grateful to the hon. Lady for welcoming the vast majority of the provisions within these clauses. She did express some concern about the breadth of the powers available to the Information Commissioner, but I point out that they are subject to a number of safeguards defining how they can be used. The commissioner is required to publish how he will exercise his powers, and that will provide organisations with clarity on the circumstances in which they are to be used.

As the hon. Lady will be aware, like other regulators, the Information Commissioner is subject to the duty under the Legislative and Regulatory Reform Act to exercise their functions

"in a way which is transparent, accountable, proportionate and consistent",

and,

"targeted only at cases in which action is needed."

There will also be a right of appeal, which is consistent with the commissioner's existing powers. On that basis, I hope that the hon. Lady is reassured.

Question put agreed to.

Clause 34 accordingly ordered to stand part of the Bill.

Clauses 35 to 38 ordered to stand part of the Bill.

Clause 39

COMPLAINTS TO CONTROLLERS

12.30 pm

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

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

Clauses 40 and 41 stand part.

That schedule 8 be the Eighth schedule to the Bill.

Sir John Whittingdale: These three clauses, together with schedule 8, streamline and clarify complaint routes for data subjects by making the respective rights and responsibilities of data controllers and data subjects clear in legislation. The measures will reduce the volume of premature complaints to the Information Commissioner, and give an opportunity to controllers to resolve complaints before they are escalated to the regulator.

Clause 39 enables data subjects to complain to a data controller if they believe that there has been an infringement of their data protection rights, and creates a duty for data controllers to facilitate the making of complaints by taking appropriate steps, such as providing a complaints form. The requirement will encourage better conversations and more dialogue between data subjects and data controllers. It will formalise best practice, and align with the standard procedures of other ombudsman services, which require complainants to seek to resolve an issue with the relevant organisation before escalation. The clause also introduces a regulation-making power for the Secretary of State to require controllers to notify the Information Commissioner of the number of complaints made to them in circumstances specified in the regulations.

Clause 40 provides the Information Commissioner with a new power to refuse to act on certain data protection complaints if certain conditions are met, specifically if the complaint has not been made to the relevant controller; the controller has not finished handling the complaint and less than 45 days have elapsed since it was made; or the complaint is considered vexatious or excessive, as defined in the Bill. For example, that could be the case with a complaint that repeats a previous complaint made by the data subject to the commissioner. The power is in addition to the discretion that the commissioner can already exercise to "take appropriate steps" to respond to a complaint and investigate it "to the extent appropriate." The clause requires the Information Commissioner to publish guidance about how it will respond to complaints and exercise its power to refuse to act on complaints. Finally, the clause also outlines the process for appeals if the commissioner refuses to act on a data protection complaint.

Clause 41 introduces schedule 8, which contains miscellaneous minor and consequential amendments to the UK General Data Protection Regulation and the Data Protection Act relating to complaints by data subjects.

Schedule 8 makes consequential amendments to the UK GDPR and the DPA relating to complaints by data subjects, which will ensure consistency across data protection legislation in relation to the changes to the complaints framework under clauses 39 and 40.

Stephanie Peacock: I will focus most of my remarks on the group on clauses 39 and 40, as clause 41 and schedule 8 contain mostly consequential provisions, as the Minister outlined.

There are two major sections to the clauses. First, they require a complainant to issue their complaint to the controller directly, through allowing the commissioner to refuse to process their complaint otherwise. Secondly, they require the commissioner to refuse any complaint that is vexatious or excessive. I will speak to both in turn.

As the ICO grows and its remit expands, given the rapidly growing use of data in our society, it makes sense that its resources should be focused where they are most needed. Indeed, when giving evidence to the Committee, the Information Commissioner and Paul Arnold of the ICO stated that their current duty to investigate all complaints is creating a burden on their resources. Therefore, the proposal to require that complainants reach out to their data controller first, before contacting the ICO, seems to make sense, as it will allow the regulator to move away from handling low-level complaints, or complaints that are under way but not yet resolved. Instead, it would be able to refocus resources into handling complaints that have been mishandled or that offer a serious threat to data rights and public trust in data use.

Though that may be seen by some businesses and controllers as shifting an extra requirement on to them, the move should be viewed overall as a positive one, as it will require controllers to have clear processes in place for handling complaints and hopefully incentivise against conducting the kind of unlawful processing that prompts complaints in the first place. Indeed, the ICO already encourages that type of best practice, with complainants often encouraged to speak directly with the relevant data controller first before seeking help from the regulator. The clause would therefore simply formalise the arrangement, providing clarity on three levels. First, it would ensure that data subjects are clear on their right to complain directly to the controller. Secondly, it would ensure that controllers are clear on their duty to respond to such complaints. Finally, the ICO would be certain of its ability to refuse a request if the complainant refuses to comply with that model.

Although it is vital that the ICO is able to modernise and direct efforts where they are most needed, it is also vital that a healthy relationship is kept between the public—as data and decision subjects—and the ICO. The public must feel that the commissioner is there to support them in exercising their rights or seeking redress where necessary, not least because lodging a complaint can already be a difficult and distressing process. Indeed, even the commissioner himself said, when he first assumed his role, that he wanted to

"make it easy for people to access remedies if things go wrong."

As such, it is pleasing to see safeguards built into the clause that ensure a complainant can still escalate their complaint to the ICO, and appeal any refusal from the commissioner to a tribunal.

Data rights groups, such as the Open Rights Group, hold much more serious concerns about the ability to refuse vexatious and excessive requests. Indeed, they worry that the new power will allow the ICO to ignore widespread and systemic abuses of data rights. As was the case with subject access requests, the difference between a complaint made in anger—which is quite likely, given that the complainant believes they have suffered an abuse

[Stephanie Peacock]

of their rights—and a vexatious one must be clearly distinguished. The ICO should not be able to reject complaints of data abuses simply because the complainant acts in ways caused by distress.

As the response of the Government to their consultation reveals, only about half of respondents agreed with the proposal to set out criteria by which the ICO can decide not to investigate a complaint. The safeguard to appeal any refusal from the commissioner is therefore crucial in ensuring that there is a clear pathway for data subjects and decision subjects to dispute the decision of the ICO. It is also right that they should be informed of that safeguard, as well as told why their complaint has been refused, and given the opportunity to complain again with a more complete picture of information.

Overall, the clauses seems to strike the right balance between ensuring safeguards for data and decision subjects while helping the ICO to modernise. However, terms such as "vexatious" and "excessive" must be clearly defined to ensure that the ICO is able to exercise this new power of refusal proportionately and sensibly.

Carol Monaghan: I am looking for some clarification from the Minister. Under clause 39, it says:

"A controller must facilitate the making of complaints…such as providing a complaint form which can be completed electronically and by other means."

Can the Minister clarify whether every data controller will have to provide an electronic means of making a complaint? For many small data controllers, which would include many of us in the room, providing an electronic means of complaint might require additional expertise and cost that they may not have. If it said, "and/or by other means", which would allow a data controller to provide a paper copy, that might provide a little more reassurance to data controllers.

Sir John Whittingdale: Let me address the point of the hon. Member for Glasgow North West first. The intention of the clause is to ensure that complainants go first to the data controller, and the data controller makes available a process whereby complaints can be considered. I certainly fully understand the concern of the hon. Lady that it should not prove burdensome, particularly for small firms, and I do not believe that it would necessarily require an electronic means to do so. If that is not the case, I will tell her, but it seems to me that the sensible approach would be for data controllers to have a process that the Information Commissioner will accept is available to complainants first, before a complaint is possibly escalated to the next stage.

With regard to the point of the hon. Member for Barnsley East, we have debated previously the change in the threshold to "vexatious" and "excessive", and we may continue to disagree on that matter.

Question put and agreed to.

Clause 39 accordingly ordered to stand part of the Bill.

Clauses 40 and 41 ordered to stand part of the Bill.

Schedule 8 agreed to.

Clause 42

CONSEQUENTIAL AMENDMENTS TO THE EITSET REGULATIONS

Amendment made: 47, Clause 42, page 72, line 12, at end insert—

"(7A) In paragraph 13 (modification of section 155 (penalty notices)), in sub-paragraph (3)(c), for "for "data subjects"" there were substituted "for the words from "data subjects" to the end".".—*(Sir John Whittingdale.)*

This amendment inserts an amendment of Schedule 2 to the EITSET Regulations which is consequential on the amendment of section 155(3)(c) of the Data Protection Act 2018 by Schedule 4 to the Bill.

Clause 42, as amended, ordered to stand part of the Bill.

Clause 43

PROTECTION OF PROHIBITIONS, RESTRICTIONS AND DATA SUBJECT'S RIGHTS

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

Sir John Whittingdale: Clause 43 is a technical measure that creates a presumption that our data protection laws should not be overridden by future laws that relate to the processing of personal data, but it respects parliamentary sovereignty by ensuring that Parliament can depart from this presumption in particular cases if it deems it appropriate to do so. For example, if new legislation permitted or required an organisation to share personal data with another for a particular purpose, the default position in the absence of any specific indication to the contrary would be that the data protection legislation would apply to the new arrangement.

Damian Collins (Folkestone and Hythe) (Con): Will my right hon. Friend confirm that the provision will also apply with trade agreements? Certainly in the early stages of the negotiations for a UK-US trade agreement, the United States Government sought to include various provisions relating to tech policy. In such a scenario, would this legislation take precedence above anything written into a trade agreement?

Sir John Whittingdale: That would certainly be my interpretation. I do not see that a trade agreement could possibly overturn an Act of Parliament unless Parliament specifically sets out that it intends that that should be the case. This is a general protection, essentially saying that in all future cases data protection legislation applies unless Parliament specifically indicates that that should not be the case.

Until now, ensuring that any new data protection measures are read consistently with the data protection legislation has relied either on inclusion of express provision to that effect in new data processing measures, or on general rules of interpretation. There are risks to that situation. Including relevant provisions in each and every new data processing provision is onerous and could be inadvertently omitted. General rules of interpretation can be open to different interpretations by courts, particularly in the light of legal challenges following our exit from the European Union. This can create the potential for legal uncertainty and as a result could lead to a less effective and comprehensive data protection legislative framework.

Clause 43 creates a presumption that any future legislation permitting the processing of personal data will be subject to the key requirements of the UK's data protection legislation unless clear provisions are made to the contrary. This is a technical but necessary measure and I commend it to the Committee.

Stephanie Peacock: I understand that the clause contains legal clarifications relating to the interaction of data protection laws with other laws. On that basis, I am happy to proceed.

Question put and agreed to.

Clause 43 accordingly ordered to stand part of the Bill.

Clause 44

REGULATIONS UNDER THE UK GDPR

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

Sir John Whittingdale: The clause outlines the process and procedure for making regulations under powers in the UK GDPR. Such provision is needed because the Bill introduces regulation-making powers into the GDPR. There is an equivalent provision in section 182 of the Data Protection Act. Among other things, the clause makes it clear that, before making regulations, the Secretary of State must consult the Information Commissioner and such other persons as they consider appropriate, other than when the made affirmative procedure applies. In such cases, the regulations can be made before Parliament has considered them, but cannot remain as law unless approved by Parliament within a 120-day period.

12.45 pm

Clause 45 introduces schedule 9, which contains a number of minor amendments to the GDPR and the Data Protection Act. Schedule 9 makes it clear that the requirements for lawful processing in articles 6 and 9 of the GDPR are cumulative. It makes technical amendments to the definition of good practice in section 124 of the Data Protection Act and other minor amendments to the Act to clarify that, in calculating the 40-day parliamentary period permitted for any objection or rejection of documents laid before Parliament, such period does not include any whole days within a period when Parliament is dissolved or prorogued, or when both Houses of Parliament are adjourned for more than four days. The amendments are minor but will improve the legal clarity of the text.

Question put and agreed to

Clause 44 accordingly ordered to stand part of the Bill.

Clause 45 ordered to stand part of the Bill.

Schedule 9 agreed to.

Clause 46

INTRODUCTORY

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

The Chair: With this it will be convenient to discuss clause 47 stand part.

Sir John Whittingdale: I am sure that the Committee will be pleased to learn that we have now completed part 1 of the Bill. [HON. MEMBERS: "Hear, hear!"]

Clause 46 provides an overview of the provisions in part 2 that are aimed at securing the reliability of digital verification services through a trust framework, a public register, an information gateway and a trust mark.

Clause 47 will require the Secretary of State to prepare and publish the digital verification services trust framework, a set of rules, principles, policies, procedures and standards that an organisation that wishes to become a certified and registered digital verification service provider must follow. The Secretary of State must consult the Information Commissioner and other appropriate persons when preparing the trust framework; that consultation requirement can be satisfied ahead of the clause coming into force. The Secretary of State must review the trust framework every 12 months and must consult the Information Commissioner and other appropriate persons when carrying out the review. I commend both clauses to the Committee.

Stephanie Peacock: Clause 46 defines digital verification services. Central to the definition, and to the framing of the debate on part 2, is the clarification that they are

"services that are provided at the request of an individual".

That is a crucial distinction: digital verification services and the kinds of digital identity that they enable are not the same as any kind of Government-backed digital ID card, let alone a compulsory one. As we will discuss, it is important that any such services are properly regulated and can be relied on. However, the clause seems to set out a sensible definition that clarifies that all such services operate at individual request and are entirely separate from universal or compulsory digital identities.

I will speak in more depth about clause 47. As we move towards an increasingly digitally focused society, it makes absolute sense that someone should be able, at their own choice, to prove their identity online as well as in the physical world. Providing for a trusted set of digital verification services would facilitate just that, allowing people to prove with security and ease who they are for purposes including opening a bank account or moving house, akin to using physical equivalents like a passport or a proof of address such as a utility bill. It is therefore understandable that the Government, building on their existing UK digital identity and attributes trust framework, want to legislate so that the full framework can be brought into law when it is ready.

In evidence to the Committee, Keith Rosser highlighted the benefits that a digital verification service could bring, using his industry of work and employment as a live case study. He said:

"The biggest impact so far has been on the speed at which employers are able to hire staff"—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 52, Q112.]

In a study of 70,000 hires, the digital identity route took an average time of three minutes and 30 seconds, saving about a week compared with having to meet with an employer in person to provide physical documents. That has benefits not only to the individuals, who can start work a week earlier, but to the wider economy, since the same people will start contributing to taxation and their local economy a week earlier too.

Secondly, Keith identified that digital verification could open up remote jobs to people living in areas where employment opportunities are harder to come by. In theory, someone living in my constituency of Barnsley East could be hired in a role that would previously have been available only in London, thanks to their ability to prove who they are without ever having to meet their employer in person.

[Stephanie Peacock]

In the light of those benefits, as well as the potential reduction in fraud from cutting down on the usability of fake documents, in principle it seems only logical to support a framework that would allow trusted digital verification services to flourish. However, the key is to ensure that the framework breeds the trust necessary to make it work. In response to the digital identity call for evidence in 2019, the Government identified that a proportion of respondents were concerned about their privacy when it came to digital verification, saying that without assurances on privacy protections it would be hard to build trust in those systems. It is therefore curious that the Government have not accompanied their framework with any principles to ensure that services are designed and implemented around user needs and that they reflect important privacy and data protection principles.

Can the Minister say why the Government have not considered placing the nine identity assurance principles on the statute book, for example, to be considered when legislating for any framework? Those principles were developed by the Government's own privacy and consumer advisory group back in 2014; they include ensuring that identity assurance can take place only where consent, transparency, multiplicity of choice, data minimisation and dispute resolution procedures are in place. That would give people the reassurance to trust that the framework is in keeping with their needs and rights, as well as those of industry.

Furthermore, can the Minister explain whether the Government intend to ensure that digital verification will not be the only option in any circumstance, making it mandatory? As Big Brother Watch points out, digital identity is not a practical or desired option, particularly for vulnerable or marginalised groups. Elderly people may not be familiar with such technology, while others might be priced out of it, especially given the recent rise in the cost of broadband and mobile bills attached to inflation. Although we must embrace the opportunities that technology can provide in identity verification, there must also be the ability to opt out and use offline methods of identification where needed, or we will risk leaving people out of participating in key activities such as jobseeking.

Finally, I look forward to hearing more about the governance of digital verification services and the framework. The Bill does not provide a statutory basis for the new office for digital identities and attributes, and there is therefore no established body for the functions related to the framework. It is important that when the new office is established, there is good communication from Government about its powers, duties, functions and funding model. After all, the framework and the principles it supports are only as strong as their enforcement.

Overall, I do not wish to stand in the way of this part of the Bill, with the caveat that I am keen to hear from the Minister on privacy protections, on the creation of the new office and on ensuring that digital verification is the beginning of a new way of verifying one's identity, not the end of any physical verification options.

Chi Onwurah: It is a pleasure to follow my hon. Friend the Member for Barnsley East. I have some general comments, which I intend to make now, on the digital verification services framework introduced and set out in clause 46. I also have some specific comments on subsequent clauses; I will follow your guidance, Mr Hollobone, if it is your view that my comments relate to other clauses and should be made at a later point.

Like my hon. Friend, I recognise the importance of digital verification services and the many steps that the Government are taking to support them, but I am concerned about the lack of coherence between the steps set out in the Bill and other initiatives, consultations and activities elsewhere in Government.

As my hon. Friend said, the Government propose to establish an office for digital identities and attributes, which I understand is not a regulator as such. It would be good to have clarity on the position, as there is no discussion in the Bill of the duties of the new office or any kind of mechanisms for oversight or appeal. What is the relationship between the office for digital identities and attributes and this legislation? The industry has repeatedly called for clarity on the issue. I think we can all agree that a robust and effective regulatory framework is important, particularly as the Bill confers broad information-gathering powers on the Secretary of State. Will the Minister set out his vision and tell us how he sees the services being regulated, what the governance model will be, how the office—which will sit, as I understand it, in the Department for Science, Innovation and Technology—will relate to this legislation, and whether it will be independent of Government?

Will the Minister also help us to understand the relationship between the digital verification services set out in the Bill and other initiatives across Government on digital identity, such as the Government Digital Service's One Login service, which we understand will be operated across Government services, and the initiatives of the Home Office's fraud strategy? Is there a relationship between them, or are they separate initiatives? If they are separate, might that be confusing for the sector? I am sure the Minister will agree that we in the UK are fortunate to have world leaders in digital verification, including iProov, Yoti and Onfido. I hope the Minister agrees that for those organisations to continue their world-leading role, they need clarification and understanding of the direction of Government and how this legislation relates to that direction.

Finally, I hope the Minister will agree that digital identity is a global business. Will he say a few words about how he has worked with, or is working with, other countries to ensure that the digital verification services model set out in this legislation is complementary to other services and interoperable as appropriate, and that it builds on the learnings of other digital verification services?

Sir John Whittingdale: I am grateful to the hon. Member for Barnsley East for setting out the Opposition's general support for the principle of moving towards the facilitation of digital verification services. She set out some of the benefits that such services can provide, and I completely echo her points on that score. I reiterate the central point that none of this is mandatory: people can choose to use digital verification services, but there is no intention to make them compulsory.

The trust framework has been set out with a wide number of principles and standards, to which privacy is central. The hon. Member for Barnsley East is right that that will be necessary to obtain trust from people seeking to use the services. She and the hon. Member for Newcastle upon Tyne Central have both set out detailed questions about the operation of the new office and the work alongside other Government Departments. I would like to respond to their points but, given that we are about to break, we could accept the general principle of this clause and then discuss them, no doubt in greater detail, in the debate on subsequent clauses. Will the Committee accept this clause with the assurance that we will address a lot of the issues just raised as we come to subsequent clauses in this part of the Bill?

Question put and agreed to.

Clause 46 accordingly ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned. —*(Steve Double.)*

1 pm

Adjourned till this day at Two o'clock.

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Sixth Sitting

Thursday 18 May 2023

(Afternoon)

CONTENTS

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 22 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
Eastwood, Mark *(Dewsbury)* (Con)
† Henry, Darren *(Broxtowe)* (Con)
† Hunt, Jane *(Loughborough)* (Con)
Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
Monaghan, Carol *(Glasgow North West)* (SNP)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
† Richards, Nicola *(West Bromwich East)* (Con)
† Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Public Bill Committee

Thursday 18 May 2023

(Afternoon)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

2 pm

Clause 47 ordered to stand part of the Bill.

Clause 48

DVS register

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

The Chair: With this it will be convenient to discuss clauses 49 to 53 stand part.

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): Clauses 48 to 52 provide the Secretary of State with powers and duties relating to the governance and oversight of digital identities in the UK. Those functions will be carried out by the office for digital identities and attributes. I can tell the hon. Member for Newcastle upon Tyne Central that the office is a team of civil servants in the Department for Science, Innovation and Technology. The office will oversee certified organisations that provide trusted digital verification services, to ensure that the purpose of the legislation is being upheld as the market develops.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): I appreciate the Minister's clarification that the office will be a group of civil servants, but I do not see that set out in the Bill, in the clause that we are currently debating. Am I wrong?

Sir John Whittingdale: As the office is an internal body, within the Department, I do not think that it would necessarily be specifically identified in the legislation in that way. If there is any more information on that, I will be happy to provide it to the hon. Lady in a letter, but the office is not a separate body to the Department.

Chi Onwurah: I thank the Minister for providing greater clarification, but if the office is not a separate body, it cannot be claimed to be independent of Government, which means that the governance of digital verification services is not independent. Will he confirm that?

Sir John Whittingdale: This is a function that will operate within Government. I do not think that it is one where there is any specific need for particular independence, but as I said, I am happy to supply further details about precisely how it will operate if that is helpful to the hon. Lady.

Let me move on from the precise operation of the body. Clause 53 sets out requirements for certified digital verification service providers in relation to obtaining top-up certificates where the Secretary of State revises and republishes the DVS trust framework.

Clause 48 provides that the Secretary of State must establish and maintain a register of digital verification service providers. The register must be made publicly available. The Secretary of State is required to add a digital verification service provider to the register, provided that it has met certain requirements. To gain a place on the register, the provider must first be certified against the trust framework by an accredited conformity assessment body. Secondly, the provider must have applied to be registered in line with the Secretary of State's application requirements under clause 49. Thirdly, the provider must pay any fee set by the Secretary of State under the power in clause 50.

The United Kingdom Accreditation Service accredits conformity assessment bodies as competent to assess whether a digital verification service meets the requirements set out in the trust framework. That, of course, is an arm's length body. Assessment is by independent audits, and successful DVS providers are issued with a certificate.

The Secretary of State is prohibited from registering a provider if it has not complied with the registration requirements. An application must be rejected if it is based on a certificate that has expired, has been withdrawn by the issuing body, or is required to be ignored under clause 53 because the trust framework rules have been amended and the provider has not obtained a top-up certificate in time. The Secretary of State must also refuse to register a DVS provider if the provider was removed from the register through enforcement powers under clause 52 and reapplies for registration while still within the specified removal period.

Clause 48(7) provides definitions for "accredited conformity assessment body", "the Accreditation Regulation", "conformity assessment body" and "the UK national accreditation body".

Clause 49 makes provision for the Secretary of State to determine the form of an application for registration in the digital verification services register, the information that an application needs to contain, the documents to be provided with an application and the manner in which an application is to be submitted.

Clause 50 allows the Secretary of State to charge providers a fee on application to be registered in the DVS register. The fee amount is to be determined by the Secretary of State. The clause also allows the Secretary of State to charge already registered providers ongoing fees. The amount and timing of those fees are to be determined by the Secretary of State.

Clauses 51 and 52 confer powers and duties on the Secretary of State in relation to the removal of persons from the register. Clause 51 places a duty on the Secretary of State to remove a provider from the register if certain conditions are met. That will keep the register up to date and ensure that only providers that hold a certificate to prove that they adhere to the standards set in the framework are included in the register. Clause 52 provides a power to the Secretary of State to remove a provider

from the register if the Secretary of State is satisfied that the provider is failing to provide services in accordance with the trust framework, or if it has failed to provide the Secretary of State with information as required by a notice issued under clause 58. Clause 52 also contains safeguards in respect of the use of that power.

Clause 53 applies where the Secretary of State revises and republishes the DVS trust framework to include a new rule or to change an existing rule and specifies in the trust framework that a top-up certificate will be required to show compliance with the new rule from a specified date.

I hope that what I have set out is reasonably clear, and on that basis I ask that clauses 48 to 53 stand part of the Bill.

Stephanie Peacock (Barnsley East) (Lab): As has been mentioned, a publicly available register of trusted digital verification services is welcome; as a result, so is this set of clauses. A DVS register of this kind will improve transparency for anyone wanting to use a DVS service, as they will be able to confirm easily and freely whether the organisation that they hope to use complies with the trust framework.

However, the worth of the register relies on the worth of the trust framework, because only by getting the trust framework right will we be able to trust those that have been accredited as following it. That will mean including enough in the framework to assure the general public that their rights are protected by it. I am thinking of things such as data minimisation and dispute resolution procedures. I hope that the Department will consider embedding principles of data rights in the framework, as has been mentioned.

As with the framework, the detail of these clauses will come via secondary legislation, and careful attention must be paid to the detail of those measures when they are laid before Parliament. In principle, however, I have no problem with the provisions of the clauses. It seems sensible to enable the Secretary of State to determine a fee for registration, to remove a person from the register upon a change in circumstances, or to remove an organisation if it is failing to comply with the trust framework. Those are all functions that are essential to the register functioning well, although any fees should of course be proportionate to keep market barriers low and ensure that smaller players continue to have access. That facilitates competition and innovation.

Similarly, the idea of top-up certificates seems sensible. Members on both sides of the House have agreed at various points on the importance of future-proofing a Bill such as this, and the digital verification services framework should have space for modernisation and adaptation where necessary. Top-up certificates will allow for the removal of any organisation that is already registered but fails to comply with new rules added to the framework.

The detail of these provisions will be analysed as and when the regulations are introduced, but I will not object to the principle of an accessible and transparent register of accredited digital verification services.

Chi Onwurah: I thank the Minister for clarifying the role of the office for digital identities and attributes. Some of the comments I made on clause 46 are probably more applicable here, but I will not repeat them, as I am sure the Committee does not want to hear them a second time. However, I ask the Minister to clarify the process. If a company objects to not being approved for registration or says that it has followed the process set out by the Secretary of State but the Secretary of State does not agree, or if a dispute arises for whatever reason, what appeal process is there, if any, and who is responsible for resolving disputes? That is just one example of the clarity that is necessary for an office of this kind.

Will the Minister clarify the dispute resolution process and whether the office for digital identities and attributes will have a regulatory function? Given the lack of detail on the office, I am concerned about whether it will have the necessary powers and resources. How many people does the Minister envisage working for it? Will they be full-time employees of the office, or will they be job sharing with other duties in his Department?

My other questions are about something I raised earlier, to which the Minister did not refer: international co-operation and regulation. I imagine there will be instances where companies headquartered elsewhere want to offer digital verification services. Will there be compatibility issues with digital verification that is undertaken in other jurisdictions? Is there an international element to the office for digital identities and attributes?

Everyone on the Committee agrees that this is a very important area, and it will only get more important as digital verification becomes even more essential for our everyday working lives. What discussions is the Minister having with the Department for Business and Trade about the kind of market that we might expect to see in digital verification services and ensuring that it is competitive, diverse and across our country?

Sir John Whittingdale: I look forward to debating the detail of the framework with the hon. Member for Barnsley East when it comes forward, but the hon. Member for Newcastle upon Tyne Central raised a couple of specific points. As I said, the new office for digital identities and attributes will be in the Department for Science, Innovation and Technology, and it will work on a similar basis to that of the office for product safety and standards, which operates within the Department for Business and Trade.

However, I should make it clear that the office for digital identities and attributes is not a regulator, because the use of digital identities is not mandatory, so it does not have investigatory or enforcement powers. It is not our intention for it to be able to levy fines or resolve individual complaints. Further down the line, as the market develops, it may be decided that it should be housed permanently in an independent body or as an arm's length body, but that is for consideration in due course. It will start off within the Department.

I will come back to the hon. Member for Newcastle upon Tyne Central with more detail about dispute resolution. I take her point; I am not sure how often what she describes is likely to happen, but clearly it is sensible at least to take account of it.

2.15 pm

Finally, the hon. Lady asked about working internationally. Obviously, the digital economy is a global phenomenon and every country will look to establish

similar types of service, so we are extremely keen to work with other countries. We are benchmarking our own framework against those of countries that will be at different stages of their digital identity development. We will also share UK expertise with anyone who wishes to learn from the lessons that we have already gained. That will be an ongoing process, but I accept that it is important that services are developed by countries on a co-operative basis globally.

Question put and agreed to.

Clause 48 accordingly ordered to stand part of the Bill.

Clauses 49 to 53 ordered to stand part of the Bill.

Clause 54

POWER OF PUBLIC AUTHORITY TO DISCLOSE INFORMATION TO REGISTERED PERSON

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

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

Clauses 55 and 56 stand part.

Government amendments 6 and 7.

Government new clause 3—*Information disclosed by the Welsh Revenue Authority*.

Government new clause 4—*Information disclosed by Revenue Scotland.*

Sir John Whittingdale: Clause 54 creates a permissive power to enable public authorities to share information relating to an individual with registered digital verification service providers. That the power is permissive means that public authorities are not under any obligation to disclose information. The power applies only where a digital verification service provider is registered in the DVS register and the individual has requested the digital verification service from that provider. Information disclosed using the power does not breach any duty of confidentiality or other restrictions relating to the disclosure of information, but the power does not enable the disclosure of information if disclosure would breach data protection legislation. The clause also gives public authorities the power to charge fees for disclosing information.

All information held by His Majesty's Revenue and Customs is subject to particular statutory safeguards relating to confidentiality. Clause 55 establishes particular safeguards for information disclosed to registered digital verification service providers by His Majesty's Revenue and Customs under clause 54. The Government will not commence measures to enable the disclosure of information held by HMRC until the commissioners for HMRC are satisfied that the technology and processes for information sharing uphold the particular safeguards relating to taxpayer confidentiality and therefore allow information sharing by HMRC to occur without adverse effect on the tax system or any other functions of HMRC.

Clause 56 obliges the Secretary of State to produce and publish a code of practice about the disclosure of information under clause 54. Public authorities must have regard to the code when disclosing information under this power. Publication of the first version of the code is subject to the affirmative resolution procedure. Publication of subsequent versions of the code is subject to the negative resolution procedure. We will work with the commissioners for HMRC to ensure that the code meets the needs of the tax system.

New clauses 3 and 4 and Government amendments 6 and 7 establish safeguards for information that reflect those already in the Bill under clause 55 for HMRC. Information held by tax authorities in Scotland and Wales—Revenue Scotland and the Welsh Revenue Authority—is subject to similar statutory safeguards relating to confidentiality. These safeguards ensure that confidence and trust in the tax system is maintained. Under these provisions, registered DVS providers may not further disclose information provided by Revenue Scotland or the Welsh Revenue Authority unless they have the consent of that revenue authority to do so. The addition of these provisions will provide an equivalent level of protection for information shared by all three tax authorities in the context of part 2 of the Bill, avoiding any disparity in the treatment of information held by different tax authorities in this context. A similar provision is not required for Northern Irish tax data, as HMRC is responsible for the collection of devolved taxes in Northern Ireland.

Stephanie Peacock: Many digital verification services will, to some extent, rely on public authorities being able to share information relating to an individual with an organisation on the DVS register. To create a permissive gateway that allows this to happen, as clause 54 does, is therefore important for the functioning of the entire DVS system, but there must be proper legal limits placed on these disclosures of information, and as ever, any disclosures involving personal data must abide by the minimisation principle, with only the information necessary to verify the person's identity or the fact about them being passed on. As such, it is pleasing to see in clause 54 the clarification of some of those legal limits, as contained in the likes of data protection legislation and the Investigatory Powers Act 2016. Similarly, clause 55 and the Government new clauses apply the necessary limits on sharing of personal data from HMRC and devolved revenue authorities under clause 54.

Finally, clause 56, which seeks to ensure that a code of practice is published regarding the disclosure of information under clause 54, will be a useful addition to the previous clauses and will ensure that the safety of such disclosures is properly considered in comprehensive detail. The Information Commissioner, with their expertise, will be well placed to help with this, so it is pleasing to see that they will be consulted during the process of designing this code. It is also good to see that this consultation will be able to occur swiftly—before the clause even comes into force—and that the resulting code will be laid before both Houses.

In short, although some disclosures of personal data from public authorities to organisations providing DVS are inevitable, as they are necessary for the very functioning of a verification service, careful attention should be paid to how this is done safely and legally. These clauses, alongside a well-designed framework—as already discussed—will ensure that that is the case.

Question put and agreed to.

Clause 54 accordingly ordered to stand part of the Bill.

Clauses 55 and 56 ordered to stand part of the Bill.

Clause 57

TRUST MARK FOR USE BY REGISTERED PERSONS

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

Sir John Whittingdale: Clause 57 makes provision for the Secretary of State to designate a trust mark to a DVS provider. The trust mark is essentially a kitemark that shows that the provider complies with the rules and standards set out in the trust framework, and has been certified by an approved conformity assessment body. The trust mark must be published by the Secretary of State and can only be used by registered digital verification service providers. The clause gives the Secretary of State powers to enforce that restriction in civil proceedings.

Stephanie Peacock: Trust marks are useful tools that allow organisations and the general public alike to immediately recognise whether or not a product or service has passed a certain testing standard or criterion. This is especially the case online, where due to misinformation and the prevalence of scams such as phishing, trust in online services can be lower than in the physical world.

The TrustedSite certification, for example, offers online businesses an earned certification programme that helps them to demonstrate that they are compliant with good business practices and maintain high safety standards. This is a benefit not only to the business itself, which is able to convert more users into clicks and sales, but to the users, who do not have to spend time researching each individual business and can explore pages and shop with immediate certainty. A trust mark for digital verification services would serve a similar purpose, enabling certified organisations that meet the trust framework criteria to be immediately recognisable, offering them the opportunity to be used by more people and offering the public assurance that their personal data is being handled by a verified source.

Of course, as is the case with this entire section of the Bill, the trust mark is only worth as much as the framework around it. Ministers should again think carefully about how to ensure that the framework supports the rights of the individual. Furthermore, the trust mark is useful only if people recognise it; otherwise, it cannot provide the immediate reassurance that it is supposed to. When the trust mark is established, what measures will the Department take to raise public awareness of it? In the same vein, to know the mark's value, the public must also be aware of the trust framework that the mark is measured against, so what further steps will the Department take to increase knowledge and understanding of digital verification services and frameworks? Finally, will the Department publish the details of any identified unlawful use of the trust mark, so that public faith in the reliability of the trust mark remains high?

Overall, the clause is helpful in showing that we take seriously the need to ensure that people do not use digital verification services that may mishandle their data.

Sir John Whittingdale: I am grateful to the hon. Lady for her support. I entirely take her point that a trust mark only really works if people know what it is and can look for it when seeking a DVS provider.

Regarding potential abuse, obviously that is something we will monitor and potentially publicise in due course. All I would say at this stage is that she raises valid points that I am sure we will consider as the new system is implemented.

Question put and agreed to.

Clause 57 accordingly ordered to stand part of the Bill.

Clause 58

POWER OF SECRETARY OF STATE TO REQUIRE INFORMATION

Amendments made: amendment 6, in clause 58, page 84, line 5, after "55" insert

"or (Information disclosed by the Welsh Revenue Authority)"

This amendment prevents the Secretary of State requesting a disclosure of information which would contravene the new clause inserted by NC3.

Amendment 7, in clause 58, page 84, line 5, after "55" insert

"or (Information disclosed by Revenue Scotland)"—*(Sir John Whittingdale.)*

This amendment prevents the Secretary of State requesting a disclosure of information which would contravene the new clause inserted by NC4.

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

The Chair: With this, it will be convenient to discuss clauses 58 and 59 stand part.

Sir John Whittingdale: Clauses 58 to 60 set out powers and duties conferred upon the Secretary of State in relation to the exercise of her governance and oversight functions under part 2.

Clause 58 enables the Secretary of State to issue a written notice that requires accredited conformity assessment bodies or registered DVS providers to provide information reasonably required by the Secretary of State to exercise functions under part 2. The notice must state why the information is required. It may also state what information is required, the form in which it should be provided, when it should be provided and the place to which it should be provided. Any notice given to a provider must also inform the provider that they may be removed from the DVS register if they fail to comply with the notice.

The power is subject to certain safeguards. Information does not have to be disclosed if to do so would breach clause 55 in relation to HMRC data or data protection legislation, or if disclosure is prohibited by the relevant parts of the Investigatory Powers Act 2016. Information does not need to be disclosed if doing so would reveal an offence that would expose a person to criminal proceedings. That does not apply to offences mentioned relating to false statements.

Clause 59 gives the Secretary of State the power to make regulations specifying that another person is able to exercise her functions under part 2. This clause enables us to move the governance and oversight functions of the Secretary of State to a third party if appropriate.

Chi Onwurah: I thank the Minister for giving way. Before he moves on to clause 60, can he set out, perhaps giving an example, where it might be appropriate to use

[Chi Onwurah]

the power in clause 59 to make arrangements for another person to take on these functions, or in what circumstances he envisages it being used?

Sir John Whittingdale: We are obviously at a very early stage in the development of this market. At the moment, it is felt right that oversight should rest with the Secretary of State, but it may be that as the market grows and develops there will need to be the oversight via a separate body. The clause keeps the power available to the Secretary of State to delegate the function if he or she chooses to do so.

Clause 60 requires the Secretary of State to publish an annual report on the functioning of this part. The first report must be published within 12 months of clause 47, the DVS trust framework clause, coming into force. The reports will help to ensure that the market continues to meet the needs of DVS providers, public authorities, regulators, civil society and individuals. I commend the clauses to the Committee.

2.30 pm

Stephanie Peacock: To oversee the DVS register, it is understandable that the Secretary of State may in some cases need to require information from registered bodies to ensure that they are complying with their duties under the framework. It is good that clause 58 provides for that power, and places reasonable legal limits on it, so that disclosures of information do not disrupt legal professional privilege or other important limitations. Likewise, it is sensible that the Secretary of State be given the statutory power to delegate some oversight of the measures in this part in a paid capacity, as is ensured by clause 59.

As I have mentioned many times throughout our scrutiny of the Bill, the Secretary of State may not always have the level of expertise needed to act alone in exercising the powers given to them by such regulations. The input of those with experience and time to commit to ensuring the quality of the regulations will therefore be vital to the success of these clauses. Again, however, we will need more information about the establishment of the OfDIA and the governance of digital identities overall to be able to interpret fully both the delegated powers and the power to require information, and how they will be used. Once again, therefore, I urge transparency from the Government as those governance structures emerge.

That leads nicely to clause 60, which requires the Secretary of State to prepare and publish yearly reports on the operation of this part. A report of that nature will offer the chance to periodically review the functioning of the trust framework, register, trust mark and all other provisions contained in this part, thereby providing an opportunity to identify and rectify any recurring issues that the system may face. That is sensible for any new project, particularly one that, through its transparency, will offer accountability of the Government to the general public, who will be able to read the published reports. In short, there are no major concerns regarding any of the three clauses, though further detail on the governance of digital identities services will need proper scrutiny.

Question put and agreed to.

Clause 58 accordingly ordered to stand part of the Bill.

Clauses 59 and 60 ordered to stand part of the Bill.

Clause 61

CUSTOMER DATA AND BUSINESS DATA

Sir John Whittingdale: I beg to move amendment 46, in clause 61, page 85, line 24, after "supplied" insert "or provided".

The definition of "business data" in clause 61 refers to the supply or provision of goods, services and digital content. For consistency with that, this amendment amends an example given in the definition so that it refers to what is provided, as well as what is supplied.

The Chair: With this it will be convenient to discuss clause stand part.

Sir John Whittingdale: We move on to part 3 of the Bill, concerning smart data usage, which I know is of interest to a number of Members. Before I discuss the detail of clause 61 and amendment 46, I will give a brief overview of this part and the policy intention behind it. The provisions in part 3 allow the Secretary of State or the Treasury to make regulations that introduce what we term "schemes" that compel businesses to share data that they hold on customers with the customer or authorised third parties upon the customer's request, and to share or publish data that they hold about the services or products that they provide. Regulations under this part will specify what data is in scope within the parameters set out by the clauses, and how it should be shared.

The rest of the clauses in this part permit the Secretary of State or the Treasury to include in the regulations the measures that will underpin these data sharing schemes and ensure that they are subject to proper safeguards—for example, relating to the enforcement of regulations; the accreditation of third party businesses wanting to facilitate data sharing; and how these schemes can be funded through levies and charging. Regulations that introduce schemes, or significantly amend existing schemes, will be subject to prior consultation and parliamentary approval through the affirmative procedure.

The policy intention behind the clauses is to allow for the creation of new smart data schemes, building on the success of open banking in the UK. Smart data schemes establish the secure sharing of customer data and contextual information with authorised third parties on the customer's request. The third parties can then be authorised by the customer to act on their behalf. The authorised third parties can therefore provide innovative services for the customer, such as analysing spending to identify cost savings or displaying data from multiple accounts in a single portal. The clauses replace existing regulation-making powers relating to the supply of customer data in sections 89 to 91 of the Enterprise and Regulatory Reform Act 2013; those powers are not sufficient for new smart data schemes to be effective.

Clause 61 defines the key terms and concepts for the powers in part 3. We have tabled a minor Government amendment to the clause, which I will explain. The definitions of data holder and trader in subsection (2) explain who may be required to provide data under the regulations. The definitions of customer data and business data deal with the two kinds of data that suppliers may

be required to provide. Customer data is information relating to the transactions between the customer and supplier, such as a customer's consumption of the relevant good or service and how much the customer has paid. Business data is wider contextual data relating to the goods or services supplied or provided by the relevant supplier. Business data may include standard prices, charges or tariffs and information relating to service performance. That information may allow customers to understand their customer data. Government amendment 46 clarifies that a specific example of business data—information about location—refers to the supply or provision of goods or services. It corrects a minor inconsistency in the list of examples of business data in subsection (2)(b).

Subsection (3) concerns who is a customer of the supplying trader, and who can therefore benefit from smart data. Customers may include both consumers and businesses. Subsection (4) enables customers to exercise smart data rights in relation to contracts they have already entered into, and subsection (5) allows the schemes to function through provision of access to data, as opposed to sending data as a one-off transfer.

Stephanie Peacock: The clause defines key terms in this part of the Bill, such as business data, customer data and data holder, as well as data regulations, customer and trader. These are key to the regulation-making powers on smart data in part 3, and I have no specific concerns to raise about them at this point.

I note the clarification made by the Minister in his amendment to the example given. As he outlined, that will ensure there is consistency in the definition and understanding of business data. It is good to see areas such as that being cleaned up so that the Bill can be interpreted as easily as possible, given its complexity to many. I am therefore happy to proceed with the Bill.

Damian Collins (Folkestone and Hythe) (Con): I rise to ask the Minister a specific question about the use of smart data in this way. A lot of users will be giving away data a device level, rather than just accessing individual accounts. People are just going to a particular account they are signed into and making transactions, or doing whatever they are doing in that application, on a particular device, but there will be much more gathering of data at the device level. We know that many companies—certainly some of the bigger tech companies—use their apps to gather data not just about what their users do on their particular app, but across their whole device. One of the complaints of Facebook customers is that if they seek to remove their data from Facebook and get it back, the company's policy is to give them back data only for things they have done while using its applications—Instagram, Facebook or whatever. It retains any device-level data that it has gathered, which could be quite significant, on the basis of privacy—it says that it does not know whether someone else was using the device, so it is not right to hand that data back. Companies are exploiting this anomaly to retain as much data as possible about things that people are doing across a whole range of apps, even when the customer has made a clear request for deletion.

I will be grateful if the Minister can say something about that. If he cannot do so now, will he write to me or say something in the future? When considering the way that these regulations work, particularly in the era of smart data when it will be far more likely that data is gathered across multiple applications, it should be clear what rights customers have to have all that data deleted if they request it.

Sir John Whittingdale: I share my hon. Friend's general view. Customers can authorise that their data be shared through devices with other providers, so they should equally have the right to take back that data if they so wish. He invites me to come back to him with greater detail on that point, and we would be very happy to do so.

Amendment 46 agreed to.

Clause 61, as amended, ordered to stand part of the Bill.

Clause 62

Power to make provision in connection with customer data

Stephanie Peacock: I beg to move amendment 112, in clause 62, page 87, line 2, at end insert—

"(3A) The Secretary of State or the Treasury may only make regulations under this section if—

(a) the Secretary of State or the Treasury has conducted an assessment of the impact the regulations may have on customers, businesses, or industry,

(b) the assessment mentioned in paragraph (a) has been published, and

(c) the assessment concludes that the regulations achieve their objective without imposing disproportionate, untargeted or unnecessary cost on customers or businesses."

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

Amendment 113, in clause 62, page 87, line 12, at end insert—

"(5) The Secretary of State or the Treasury may invite a relevant sectoral regulator to contribute to, or to conduct, any impact assessment conducted in order to enable the Secretary of State or the Treasury to fulfil their obligation under subsection (4)."

This amendment would allow the Secretary of State or the Treasury to enable a relevant sectoral regulator to contribute to, or conduct, any impact assessments on smart data regulations.

Amendment 114, in clause 62, page 87, line 12, at end insert—

"(5) The Secretary of State or the Treasury must consult representatives of the relevant business or industry sector to inform their decision whether to make regulations under this section."

This amendment would require the Secretary of State or the Treasury to consult representatives of the relevant business or industry sector before making smart data regulations.

Amendment 115, in clause 62, page 87, line 12, at end insert—

"(5) Within six months of the passage of this Act, the Secretary of State must—

(a) publish a target date for the coming into force of the first regulations under this section, and

(b) make arrangements for the completion of an assessment of the impact of those regulations."

This amendment would require Government to identify a target for a first smart data scheme within 6 months, and make arrangements for an impact assessment for these regulations.

Stephanie Peacock: Of all the provisions in the Bill, the ones on smart data are those that I am most excited about and pleased to welcome. The potential of introducing smart data schemes is immense: they can bring greater choice to consumers, enable innovation, increase competition and result in the delivery of better products and services. I will address amendments 112 and 113, but I look forward to the opportunity to speak in support of this part more widely.

Most of the detail on how and where smart regimes will be regulated in practice through this Bill will follow in secondary legislation and regulation. That is deliberate and welcome, as it ensures that smart data schemes are built around the realities of the sectors to which they apply. Given that they cannot be included on the face of the Bill, however, it is important that the regulations are prepared in the way that any good data-related law is. There must be a committee of consultation to ensure that the outcome works effectively for consumers and businesses, with the appropriate data protection safeguards.

Indeed, there may be certain sectors in which the costs simply outweigh the benefits of introducing such a regime. Sky believes that there is currently no evidence that a smart data scheme in the communications sector would bring clear and tangible additional benefits to customers. Ofcom consulted on the proposal in 2020 and came to a similar conclusion. Sky argues that the communications sector already has

"a very high bar for supporting consumers to use data to find the best deal for them. For example, in 2020 Ofcom introduced End of Contract Notifications",

which tell customers when their current contract is ending and what they could save by signing up to another deal. Sky says that Ofcom is

"also in the process of introducing One Touch Switching for fixed broadband which will make it easier for customers to move between providers who operate on different networks".

As BT identifies, smart data initiatives require significant time and investment to implement. The Government's impact assessment estimates that the implementation cost for the telecoms sector for a smart data initiative could be anywhere between £610 million and £732 million. That is not to say that the cost outweighs the potential benefits for all industries, including telecoms, but it is important that the Government weigh that up before making any regulations, particularly given that large costs be passed on to consumers, or that there may be less investment in other areas. In the telecoms industry, it could lead to a reduction in investment in full-fibre broadband and 5G. It is imperative, therefore, to ensure that all costs remain targeted, proportionate and necessary to bring about an overall benefit that outweighs the costs. An impact assessment would provide assurance that this has been taken into consideration before any new schemes are introduced.

When conducting such an assessment, sectoral regulators, which can provide expert insight into the impact of smart data in any particular industry, will be well placed to assess the costs and benefits in the detail needed. That is something the Government themselves recognise, as they have placed a requirement in the Bill to consult those regulators. The amendments I propose would strengthen that commitment, allowing relevant sectoral regulators the opportunity, where appropriate, to be formally involved in the process of conducting an impact assessment.

2.45 pm

Moving to amendment 114, smart data initiatives are incredibly complex to run, let alone implement in the first place. As BT argues, for example, a working regime will require steps to guarantee the security, interoperability, quality, intelligibility and comparability of sensitive data across different industry actors. For that to come to fruition, Government must work to establish a collaborative relationship with sectoral regulators and industry. Only then will they be able to work together to co-create a functioning smart scheme that provides solutions that actually benefit consumers. Inserting a requirement to consult industry when conducting an impact assessment would allow that kind of collaboration to be built into the process from the very beginning, giving them a meaningful say on how their industry might be impacted and what the potential challenges of implementation might be. If the Minister does not intend to accept the amendment, will he tell us what steps will his Department take to foster collaborative relationships between Government, regulators and industry before making regulations for any smart data schemes?

Turning to amendment 115, although we must be cautious to ensure that smart data is being implemented where it is actually beneficial—hence the requirement to conduct impact assessments—if the UK is to be a frontrunner in capitalising on the possibilities of smart data, we must act quickly. At the moment, however, although this part lays the foundations for the Secretary of State to regulate for a smart data regime, there is no obligation on them to do so, or even to explore the option of doing so. The amendment would ensure that this opportunity does not get forgotten within the busy day-to-day operations of the Department by ensuring that a target for a data scheme is identified within six months.

That absolutely does not mean that any regulations themselves will have to be made, but it would encourage the Government to actually act on this part and to state an intention to explore the potential of smart data within a certain sector. Arrangements could be made to conduct a proper impact assessment to analyse whether this would be beneficial. There will be no real benefit from this part if it is left unused. It is vital that we capture the moment and enable smart data where it can boost our economy and the consumer experience.

Sir John Whittingdale: I assure the hon. Lady that I and, no doubt, the whole Committee share her excitement about the potential offered by smart data, and I have sympathy for the intention behind her amendments. However, taking each one in turn, we feel amendment 112 is unnecessary because the requirements are already set by the better regulation framework, the Small Business, Enterprise and Employment Act 2015 and, indeed, these clauses. Departments will conduct an impact assessment in line with the better regulation framework and Green Book guidance when setting up a new smart data scheme, and must demonstrate consideration of their requirements under the Equality Act 2010. That will address the proportionality, targeting and necessity of the scheme.

Moreover, the clauses require the Government to consider the effect of the regulations on matters including customers, businesses and competition. An impact assessment would be an effective approach to

meeting those requirements. However, there is a risk that prescribing exactly how a Department should approach the requirements could unnecessarily constrain the policymaking process.

I turn to amendment 113. Clause 74(5) already requires the Secretary of State or the Treasury to consult with relevant sector regulators as they consider appropriate. As part of the process, sector regulators may be asked to contribute to the development of regulatory impact assessments, so we do not believe the amendment is necessary.

On amendment 114, we absolutely share the view of the importance of Government consulting businesses before making regulations. That is why, under clause 74(6), the Secretary of State or the Treasury must, when introducing a smart data scheme, consult such persons as are likely to be affected by the regulations and such sectoral regulators as they consider appropriate. Those persons will include businesses relevant to the envisaged scheme.

On amendment 115, we absolutely share the ambition to grab whatever opportunities smart data offers. In particular, I draw the hon. Lady's attention to the commitments made last month by the Economic Secretary to the Treasury, who set out the Treasury's plans to use the smart data powers to provide open banking with a sustainable regulatory framework, while the Under-Secretary of State for Business and Trade, my hon. Friend the Member for Thirsk and Malton (Kevin Hollinrake), chaired the inaugural meeting of the Smart Data Council last month. That council has been established to support and co-ordinate the development of smart data schemes in a timely manner.

With respect to having a deadline for schemes, we should recognise that implementation of the regulations requires careful consideration. The hon. Member for Barnsley East clearly recognises the importance of consultation and of properly considering the impacts of any new scheme. We are committed to that, and there is a risk that a statutory deadline for making the regulations would jeopardise our due diligence. I assure her that all her concerns are ones that we share, so I hope that she will accept that the amendments are unnecessary.

Stephanie Peacock: I am grateful to the Minister for those assurances. I am reassured by his comments, and I am happy to beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

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

The Chair: With this it will be convenient to discuss clause 63 stand part.

Sir John Whittingdale: Clause 62 provides the principal regulation-making power to establish smart data schemes in relation to customer data. The clause enables the Secretary of State or the Treasury to make regulations that require data holders to provide customer data either directly to a customer, or to a person they have authorised, at their request. Subsection (3) of the clause also allows for an authorised person who receives the customer data, to exercise the customer's rights in relation to their data on their behalf. We call that "action initiation".

An illustrative example could be in open banking, where customers can give authorised third parties access to their data to compare the consumer's current bank account with similar offers, or to group the contracts within a household together for parents or guardians to better manage children's accounts. Subsection (3) could allow the authorised third party to update the customer's contact details across the associated accounts, for example if an email address changes.

Clause 63 outlines the provisions that smart data scheme regulations may contain when relating to customer data. The clause establishes much of the critical framework that smart data schemes will be built on. On that basis, I commend clauses 62 and 63 to the Committee.

Stephanie Peacock: As previously mentioned, and with the caveats that I expressed when I was discussing my amendments, I am extremely pleased to be able to welcome this part of the Bill. In essence, clauses 62 and 63 enable regulations that will allow for customer data to be provided to a third party on request. I will take the opportunity to highlight why that is the case by looking at some of the benefits that smart data can provide.

Since 2018, open banking—by far the most well known and advanced version of smart data in operation—has demonstrated what smart data can deliver over and over again. For the wider economy, the benefits have been remarkable, with the total value to the UK economy now amounting to more than £4.1 billion, according to Coadec, the Coalition for a Digital Economy. Consumers' experience of banking has been revolutionised if they have consented of their own accord to have third-party applications access their financial data.

Indeed, a whole host of money management tools and apps can now harness people's financial data to create personalised recommendations based on their spending habits, including how to budget or save. During a cost of living crisis, some of those tools have been extremely valuable in helping people to manage new bills and outgoings. Furthermore, online retailers can now connect directly to someone's bank so that, rather than spending the time filling in their card details each time they make a purchase, an individual can approve the transaction via their online banking system.

It is important to reiterate that open banking is based on consent, so consumers participate only if they feel it is right for them. As it happens, millions of people have capitalised on the benefits. More than seven million consumers and 50% of small and medium-sized enterprises have used open banking services to gain a holistic view of their finances, to support applications for credit and to pay securely, quickly and cheaply.

Though open banking has brought great success for both consumers and the wider economy, it is also important that the Government learn lessons from its implementation. We must pay close attention to how the introduction of open banking has impacted both the industry and consumers and ensure that any takeaways are factored in when considering an expansion of smart data into new industries.

Further, given that the Government clearly recognise the value of open data, as shown by this section of the Bill, it is a shame that the Bill does not go further in exploring the possibilities of opening datasets in other

[Stephanie Peacock]

settings. Labour has explicitly set out to do that in its industrial strategy. For example, we have identified that better, more open datasets on jobs could help us to understand where skills shortages are, allowing jobseekers, training providers and Government to better fill those gaps.

The provisions in clauses 62 and 63 to create new regimes of smart data are therefore welcome, but the Bill unfortunately remains a missed opportunity to fully capitalise on the opportunities of open, secure data flows.

Question put and agreed to.

Clause 62 accordingly ordered to stand part of the Bill.

Clause 63 ordered to stand part of the Bill.

Clause 64

POWER TO MAKE PROVISION IN CONNECTION WITH BUSINESS DATA

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

The Chair: With this it will be convenient to consider clause 65 stand part.

Sir John Whittingdale: Clause 64 provides the principal regulation-making power for the creation of smart data schemes relating to business data. Regulations created through this clause allow for business data to be provided to the customer of a trader or a third-party recipient. Business data may also be published to be more widely available.

These regulations relating to business data will increase the transparency around the pricing of goods and services, which will increase competition and benefit both consumers and smaller businesses. To give just one example, the Competition and Markets Authority recently highlighted the potential of an open data scheme that compared the prices of fuel at roadside stations, increasing competition and better informing consumers. It is that kind of market intervention that the powers provide for.

Clause 65 outlines provisions that regulations relating to business data may contain. Those provisions are non-exhaustive. The clause largely mirrors clause 63, extending the same protections and benefits to schemes that make use of businesses data exclusively or in tandem with customer data. The clause differs from clause 63 in subsection (2), where an additional consideration is made as to who may make a request for business data. As action initiation relates only to an authorised person exercising a customer's rights relating to their data, clause 65 does not include the references to that that are made in subsections (7) and (8) of clause 63.

Stephanie Peacock: The measures in these clauses largely mirror 62 and 63, but they refer to business data rather than customer data. I therefore refer back to my comments on clause 62 and 63 and the benefits that new regulations such as these might be able to provide. Those remarks provide context as to why I am pleased to support these measures, which will allow the making of regulations that require data holders to share business data with third parties.

However, I would like clarification from the Minister on one point. The explanatory notes explain that the powers will likely be used together with those in clauses 62 and 63, but it would be good to hear confirmation from the Minister on whether there may be circumstances in which the Department envisages using the powers regarding business data distinctly. If there are, will he share examples of those circumstances? It would be good for both industry and Members of this House to have insight into how these clauses, and the regulatory powers they provide, will actually be used.

Sir John Whittingdale: I think it is probably sensible if I come back to the hon. Lady on that point. I am sure we would be happy to provide examples if there are ones that we can identify.

Question put and agreed to.

Clause 64 accordingly ordered to stand part of the Bill.

Clause 65 ordered to stand part of the Bill.

Clause 66

DECISION-MAKERS

3 pm

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

The Chair: With this it will be convenient to discuss Clauses 67 to 72 stand part.

Sir John Whittingdale: Clauses 66 to 72 contain a number of provisions that will allow smart data regulations to function effectively. They are provisions on decision makers who approve and monitor third parties that can access the data, provisions on enforcement of the regulations and provisions on the funding of smart data schemes. It is probably sensible that I go through each one in more detail.

Clause 66 relates to the appointment of persons or accrediting bodies referred to as decision makers. The decision makers may approve the third parties that can access customer and business data, and act on behalf of customers. The decision makers may also revoke or suspend their accreditation, if that is necessary. An accreditation regime provides certainty about the expected governance, security and conduct requirements for businesses that can access data. Customers can be confident their chosen third party meets an appropriate standard. Clause 66 allows the decision maker to monitor compliance with authorisation conditions, subject to safeguards in clause 68.

Clause 67 enables regulations to confer powers of enforcement on a public body. The public body will be the enforcer, responsible for acting upon any breaches of the regulations. We envisage that the enforcer for a smart data scheme is likely to be an existing sectoral regulator, such as the Financial Conduct Authority in open banking. While the clause envisages civil enforcement of the regulations, subsection (6) allows for criminal offences in the case of falsification of information or

evidence. Under subsections (3) and (10), the regulations may confer powers of investigation on the enforcer. That may include powers to require the provision of information and powers of entry, search and seizure. Those powers are subject to statutory restrictions in clause 68.

Clause 68 contains provisions limiting the investigatory powers given to enforcers. The primary restriction is that regulations may not require a person to give an enforcer information that would infringe the privileges of Parliament or undermine confidentiality, legal privilege and, subject to the exceptions in subsection (7), privilege against self-incrimination. Subsection (8) prevents any written or oral statement given in response to a request for information in the course of an investigation from being used as evidence against the person being prosecuted for an offence, other than that created by the data regulations.

Clause 69 contains provisions relating to financial penalties and the relevant safeguards. It sets out what regulations must provide for if enabling the use of financial penalties. Subsection (2) requires that the amount of a financial penalty is specified in, or determined in accordance with, the regulations. For example, the regulations may set a maximum financial penalty that an enforcer can impose and they may specify the methodology to be used to determine a specific financial penalty.

Clause 70 enables actors in smart data schemes to require the payment of fees. The circumstances and conditions of the fee charging process will be specified in the regulations. The purpose of the clause, along with clause 71, is to seek to ensure that the costs of smart data schemes, and of bodies exercising functions under them, can be met by the relevant sector.

It is intended that fees may be charged by accrediting bodies and enforcers. For example, regulations could specify that an accrediting body may charge third parties to cover the cost of an accreditation process and ongoing monitoring. Enforcers may also be able to charge to cover or contribute to the cost of any relevant enforcement activities. The regulations may provide for payment of fees only by persons who are directly affected by the performance of duties, or exercise of powers, under the regulations. That includes data holders, customers and those accessing customer and business data.

Clause 71 will enable the regulations to impose a levy on data holders or allow a specified public body to do so. That is to allow arrangements similar to those in section 38 of the Communications Act 2003, which enables the fixing of charges by Ofcom. Together with the provision on fees, the purpose of the levy is to meet all or part of the costs incurred by enforcers and accrediting bodies, or persons acting on their behalf. The intention is to ensure that expenses can be met without incurring a cost to the taxpayer. Levies may be imposed only in respect of data holders that appear to be capable of being directly affected by the exercise of the functions.

Clause 72 provides statutory authority for the Secretary of State or the Treasury to give financial assistance, including to accrediting bodies or enforcers. Subsection (2) provides that the assistance may be given on terms and conditions that are deemed appropriate by the regulation maker. Financial assistance is defined to include both actual or contingent assistance, such as a grant, loan, guarantee or indemnity. It does not include the purchase of shares. I commend clauses 66 to 72 to the Committee.

Stephanie Peacock: Clauses 66 to 72 provide for decision makers and enforcers to help with the operation and regulation of new smart data regimes. As was the case with the digital verification services, where I agreed that there was a need for the Secretary of State to have limited powers to ensure compliance with the trust framework, powers will be needed to ensure that any regulations made under this part of the Bill are followed. The introduction in clause 67 of enforcers—public bodies that will, by creating fines, penalties and notices of compliance, ensure that organisations follow regulations made under part 3—is therefore welcome.

As ever, it is pleasing to see that the relevant restrictions on the powers of enforcers are laid out in clause 68, to ensure that they cannot infringe upon other, more fundamental rights. It is also right, as is ensured by clause 69, that there are safeguards on the financial penalties that an enforcer is able to issue. Guidance on the amount of any penalties, as well as a formalised process for issuing notices and allowing for appeal, will provide uniformity across the board so that every enforcer acts proportionately and consistently.

Decision makers allowed for by clause 66 will be important, too, in conjunction with enforcers. They will ensure there is sufficient oversight of the organisations that are enabled to have access to customer or business data through any particular smart data regimes. Clauses 70, 71 and 72, which finance the activities of decision makers and enforcers, follow the trend of sensible provisions that will be required if we are to have confidence that regulations made under this part of the Bill will be adhered to. In short, the measures under this grouping are largely practical, and they are necessary to support clauses 62 to 65.

Question put and agreed to.

Clause 66 accordingly ordered to stand part of the Bill.

Clauses 67 to 72 ordered to stand part of the Bill.

Clause 73

CONFIDENTIALITY AND DATA PROTECTION

Question proposed, That the clause stand part of the Bill

The Chair: With this it will be convenient to discuss clauses 74 to 77 stand part.

Sir John Whittingdale: Clauses 73 to 77 relate to confidentiality and data protection; various provisions connected with making the regulations, including consultation, parliamentary scrutiny and a duty to conduct periodic reviews of regulations; and the repeal of the existing regulation-making powers that these clauses replace.

Clause 73(1) allows the regulations to provide that there are no contravening obligations of confidence or other restrictions on the processing of information. Subsection (2) ensures that the regulations do not require or authorise processing that would contravene the data protection legislation. The provisions are in line with

[Sir John Whittingdale]

the approach taken towards pension dashboards, which are electronic communications services that allow individuals to access information about their pensions.

Clause 74(1) allows the regulation-making powers to be used flexibly. Subsection (1)(f) allows regulations to make provision by reference to specifications or technical requirements. That is essential to allow for effective and safe access to customer data, for instance the rapid updating of IT and security requirements, and it mirrors the powers enacted in relation to pensions dashboards, which I have mentioned. Clause 74(2) provides for limited circumstances in which it may be necessary for regulations to modify primary legislation to allow the regulations to function effectively. For instance, it may be necessary to extend a statutory alternative dispute resolution scheme in a specific sector to cover the activities of a smart data scheme.

Clause 74(3) states that affirmative parliamentary scrutiny will apply to the first regulations made under clauses 62 or 64; that is, affirmative scrutiny will apply to regulations that introduce a scheme. Affirmative parliamentary scrutiny will also be required where primary legislation is modified, where regulations make requirements more onerous for data holders and where the regulations confer monitoring or enforcement functions or make provisions for fees or a levy. Under clause 74(5), prior to making regulations that will be subject to affirmative scrutiny, the Secretary of State or the Treasury must consult persons who are likely to be affected by the regulations, and relevant sectoral regulators, as they consider appropriate.

The Government recognise the importance of enabling the ongoing scrutiny of future regulations, so clause 75 requires the regulation maker to review the regulations at least at five-yearly intervals. Clause 76 repeals the regulation-making powers in sections 89 to 91 of the Enterprise and Regulatory Reform Act 2013, which are no longer adequate to enable the introduction of effective smart data schemes. Those sections are replaced by the clauses in part 3 of the Bill. Clause 77 defines, or refers to definitions of, terms used in part 3 and is essential to the functioning and clarity of part 3. I commend the clauses to the Committee.

Stephanie Peacock: Many of the clauses in this grouping are supplementary to the provisions that we have already discussed, or they provide clarification as to which regulations under part 3 are subject to parliamentary scrutiny. I have no further comments to add on the clauses, other than to welcome them as fundamental to the wider part. However, I specifically welcome clause 75, which requires that the regulations made under this part be periodically reviewed at least every five years.

I hope that such regulations will be under constant review on an informal basis to assess how well they are working, but it is good to see a formal mechanism to ensure that that is the case over the long term. It would have been good, in fact, to see more such provisions throughout the Bill, to ensure that regulations that are made under it work as intended. Overall, I hope it is clear that I am very supportive of this part's enabling of smart data regimes. I look forward to it coming into force and unlocking the innovation and consumer benefits that such schemes will provide.

Question put and agreed to.

Clause 73 accordingly ordered to stand part of the Bill.

Clause 74 to 77 ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned. *—(Steve Double.)*

3.14 pm

Adjourned till Tuesday 23 May at twenty-five minutes past Nine o'clock.

Written evidence reported to the House

DPDIB29 Connected by Data (supplementary submission)

DPDIB30 Reset

DPDIB31 Professor David Erdos, Professor of Law and the Open Society, Co-Director, Centre for Intellectual Property and Information Law, Faculty of Law, University of Cambridge

DPDIB32 Kent & Medway Health and Care Strategic Information Governance Network

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Seventh Sitting

Tuesday 23 May 2023

(Morning)

CONTENTS

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 27 May 2023

The Committee consisted of the following Members:

Chairs: Mr Philip Hollobone, † Ian Paisley

Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Eastwood, Mark *(Dewsbury)* (Con)
† Henry, Darren *(Broxtowe)* (Con)
Hunt, Jane *(Loughborough)* (Con)
Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Monaghan, Carol *(Glasgow North West)* (SNP)
Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
† Richards, Nicola *(West Bromwich East)* (Con)
† Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 23 May 2023

(Morning)

[Ian Paisley *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

9.25 am

Stephanie Peacock (Barnsley East) (Lab): On a point of order, Mr Paisley. I would like to correct the record regarding my comments on clause 13, which appear in column 148 of the Committee proceedings in *Hansard* for Tuesday 16 May. I referred to the views of Lexology and included a quote, which I attributed to that organisation, when in fact the views and quote in question were those of an organisation named Prighter, which were simply published by Lexology.

The Chair: Thank you for that clarification.

Clause 78

The PEC Regulations

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): I beg to move amendment 5, in clause 78, page 100, line 30, after "86" insert "and [Codes of conduct]".

This amendment is consequential on NC2.

The Chair: With this it will be convenient to discuss Government new clause 1 and Government new clause 2.

Sir John Whittingdale: It is a pleasure to serve under your chairmanship, Mr Paisley. Welcome to the Committee.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 place specific requirements on organisations in relation to use of personal data in electronic communications. They include, for example, rules on the use of emails, texts and phone calls for direct marketing purposes and the use of cookies and similar technologies.

Trade associations have told us that sometimes their members need guidance on complying with the legislation that is more bespoke than the general regulatory guidance from the Information Commissioner's Office. New clause 2 will allow representative bodies to design codes of conduct on complying with the PEC regulations that reflect their specific processing operations. There are already similar provisions in articles 40 and 41 of the UK General Data Protection Regulation to help organisations in particular sectors to comply.

Importantly, codes of conduct prepared under these provisions can be contained in the same document as codes of conduct under the UK GDPR. That will be particularly beneficial to representative bodies that are developing codes for processing activities that are subject to the requirements of both the UK GDPR and the PEC regulations. New clause 2 envisages that representative bodies will draw up voluntary codes of conduct and then seek formal approval of them from the Information Commissioner. The Information Commissioner will approve a code only if it contains a mechanism for the representative body to monitor their members' compliance with the code.

New clause 1 makes a related amendment to article 41 of the UK GDPR to clarify that bodies accredited to monitor compliance with codes of conduct under the GDPR are required to notify the Information Commissioner only if they suspend or exclude a person from a code. Government amendment 5 is a minor and technical amendment necessary as a consequence of new clause 2.

These provisions are being put into the Bill at the suggestion of business organisations. We hope that they will allow organisations to comply more easily with the requirements.

Stephanie Peacock: It is a pleasure to serve under your chairship, Mr Paisley, and I too welcome you to the Committee.

As I have said more than once in our discussions, in many cases the burden of following regulations can be eased just as much by providing clarification, guidance and support as by removing regulation altogether. I advocated for codes of practice in more detail in the discussion of such codes in the public sector, under clause 19, and during our debates on clauses 29 and 30, when we were discussing ICO codes more generally. New clauses 1 and 2 seem to recognise the value of codes of practice too, and both seek to provide either clarification or the sharing of best practice in terms of following the PEC regulations. I have no problem with proceeding with the Bill with these inclusions.

Amendment 5 agreed to.

Sir John Whittingdale: I beg to move amendment 48, in clause 78, page 100, line 30, after "86" insert "and [Pre-commencement consultation]".

This amendment is consequential on NC7.

The Chair: With this it will be convenient to discuss Government new clause 7.

Sir John Whittingdale: New clause 7 clarifies that the consultation requirements imposed by the Bill in connection with or under the PEC regulations can be satisfied by consultation that takes place before the relevant provision of the Bill comes into force. That ensures that the consultation work that supports development of policy before the Bill is passed can continue and is not paused unnecessarily. A similar provision was included in section 182 of the Data Protection Act 2018. Government amendment 48 is a minor and technical amendment which is necessary as a consequence of new clause 7. I commend the new clause and amendment to the Committee.

Stephanie Peacock: The new clause and accompanying amendment seek to expedite work on consultation in relation to the measures in this part. It makes sense that

consultation can begin before the Bill comes into force, to ensure that regulations can be acted on promptly after its passing. I have concerns about various clauses in this part, but no specific concerns about the overarching new clause, and am happy to move on to discussing the substance of the clauses to which it relates.

Amendment 48 agreed to.

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

Sir John Whittingdale: Clause 78 introduces part 4 of the Bill, which amends the Privacy and Electronic Communications (EC Directive) Regulations 2003. Clauses 79 to 86 refer to them as "the PEC Regulations" for short. They sit alongside the Data Protection Act and the UK GDPR. We will debate some of the more detailed provisions in the next few clauses.

Question put and agreed to.

Clause 78, as amended, accordingly ordered to stand part of the Bill.

Clause 79

STORING INFORMATION IN THE TERMINAL EQUIPMENT OF A SUBSCRIBER OR USER

Stephanie Peacock: I beg to move amendment 116, in clause 79, page 101, line 15, leave out

"making improvements to the service"

and insert

"making changes to the service which are intended to improve the user's experience".

Cookies are small text files that are downloaded on to somebody's computer or smartphone when they access a website; they allow the website to recognise the person's device, and to store information about the user's preferences or past actions. The current rules around using cookies, set out in regulation 6 of the PEC regulations, dictate that organisations must tell people that the cookies are there, explain what the cookies are doing and why, and finally get the person's freely given, specific and informed consent to store cookies on their device. However, at the moment there is almost universal agreement that the system is not working as intended.

To comply with the legislation, most website have adopted what is known as a cookie banner—a notice that pops up when a user first visits the site, prompting them to indicate which cookies they are happy with. However, due to the sheer volume of those banners, in many cases people no longer feel they are giving consent because they are informed or because they freely wish to give it, but are doing so simply because the banners stop them using the website as they wish.

In their communications regarding the Bill, the Government have focused on reducing cookie fatigue, branding it one of the headline achievements of the legislation. Unfortunately, as I will argue throughout our debates on clause 79, I do not believe that the Bill will fix the problem in the way that users hope. The new exemptions to the consent requirement for purposes that present a low risk to privacy may reduce the number of circumstances in which permission might be required, but there will still be a wide-ranging list of circumstances where consent is still required.

If the aim is to reduce cookie fatigue for users, as the Government have framed the clause, the exemptions must centre on the experience of users. If they do not, the clause is not about reducing consent fatigue, but rather about legitimising large networks of online surveillance of internet users. With that in mind, amendment 116 would narrow the exemption for collecting statistical information with a view to improving a service so that it is clear that any such improvements are exclusively considered to be those from the user's perspective. That would ensure that the term "improvements" cannot be interpreted as including sweeping changes for commercial benefit, but is instead focused only on benefits to users.

I will speak to proposed new regulation 6B when we debate later amendments, but I reiterate that I have absolute sympathy for the intention behind the clause and want as much as anyone to see an end to constant cookie banners where possible. However, we must place the consumer and user experience at the heart of any such changes. That is what we hope to ensure through the amendment, with respect to the list of exemptions.

Sir John Whittingdale: I am grateful to the hon. Lady for making it clear that the Opposition share our general objective in the clause. As she points out, the intention of cookies has been undermined by their ubiquity when they are placed as banners right at the start. Clause 79 removes the requirement to seek consent for the placement of audience measurement cookies. That means, for example, that a business could place cookies to count the number of visitors to its website without seeking the consent of web users via a cookie pop-up notice. The intention is that the organisation could use the statistical information collected to understand how its service is being used, with a view to improving it. Amendment 116 would mean that "improvements to the service" would be narrowed in scope to mean improvements to the user's experience of the service, but while that is certainly one desirable outcome of the new exception, we want it to enable organisations to make improvements for their own purposes, and these may not necessarily directly improve the user's experience of the service.

Organisations have repeatedly told us how important the responsible use of data is for their growth. For example, a business may want to use information collected to improve navigation of its service to improve sales. It could use the information collected to make improvements to the back-end IT functionality of its website, which the user may not be aware of. Or it could even decide to withdraw parts of its service that had low numbers of users; those users could then find that their experience was impaired rather than improved, but the business could invest the savings gained to improve other parts of the service. We do not think that businesses should be prevented from improving services in this way, but the new exception provides safeguards to prevent them from sharing the collected data with anyone else, except for the same purpose of making improvements to the service. On that basis, I hope the hon. Lady will consider withdrawing her amendment.

Stephanie Peacock: I am grateful for the Minister's answer. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Sir John Whittingdale: I beg to move amendment 49, in clause 79, page 102, leave out lines 21 to 23.

Clause 79 amends regulation 6 of the PEC Regulations to create new exceptions from the prohibition on storing and accessing information in terminal equipment. New paragraph (2C) contains an exception for software updates that satisfy specified requirements. This amendment removes a requirement that the subscriber or user can object to the update and does not object.

The Chair: With this it will be convenient to discuss Government amendments 50 to 54.

Sir John Whittingdale: Clause 79 reforms regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003, which sets the rules on when an organisation can store information or gain access to information stored on a person's device—for example, their computer, phone or tablet. This is commonly described as the cookies rule, but it includes similar technologies such as tracking pixels and device fingerprinting. Currently, organisations do not have to seek a user's consent to place cookies that are strictly necessary to provide a service requested by the user—for example, to detect fraud or remember items in a user's online shopping basket.

To reduce the number of cookie pop-up notices that can spoil web users' enjoyment of the internet, clause 79 will remove the requirement for organisations to seek consent for several low privacy risk purposes, including the installation of software updates necessary for the security of the device. Government amendments 49 and 51 remove the user's right to opt out of the software security update and the right to remove an update after it has taken effect. Government amendment 50 removes the right to disable an update before it takes effect.

Although these measures were initially included in the Bill to give web users a choice about whether security updates were installed, stakeholders have subsequently advised us that the failure to install certain updates could result in a high level of risk to the security of users' devices and personal information. We have been reflecting on the provisions since the Bill was introduced, and have concluded that removing them is the right thing to do, in the interests of security of web users. Even if these provisions are omitted, organisations will still need to provide users with clear and comprehensive information about the purpose of software security updates. Web users will also still have the right to postpone an update for a limited time before it takes effect.

Government amendment 54 concerns the regulation-making powers under the new PEC regulations. One of the main aims is to ensure that web users are empowered to use automated technology such as browsers and apps to select their choices regarding which cookies they are willing to accept. The Secretary of State could use powers under these provisions to require consent management tools to meet certain standards or specifications. so that web users can make clear, meaningful choices once and have those choices respected throughout their use of the internet.

The Committee will note that new regulation 6B already requires the Secretary of State to consult the Information Commissioner and other interested parties before making any new regulations on consent management tools. Government amendment 54 adds the Competition and Markets Authority as a required consultee. That will help ensure that any competition impacts are properly considered when developing new regulations that set standards of design.

Finally, Government amendments 52 and 53 make minor and technical changes that will ensure that future regulations made under the reformed PEC regulations can include transitional, transitory or savings provisions. These will simply ensure there is a smooth transition to the new regime if the Secretary of State decides to make use of these new powers. I commend the amendments to the Committee.

Stephanie Peacock: I understand that amendments 49 to 51 primarily remove the option for subscribers or users to object to or disable an update or software for security reasons. As techUK has highlighted, the PEC regulations already contain an exemption on cookie consent for things that are strictly necessary, and it was widely accepted that security purposes met this exemption. This is reflected by its inclusion in the list of things that meet the criteria in new paragraph (5).

However, in the Bill the Government also include security updates in the stand-alone exemption list. This section introduces additional conditions that are not present in the existing law, including the requirement to offer users an opt-out from the security update and the ability to disable or postpone it. The fact that this overlap has been clarified by removing the additional conditions seems sensible. Although user choice has value, it is important that we do not leave people vulnerable to known security flaws.

In principle, Government amendment 54 is a move in the right direction. I will speak to regulation 6B in more detail when we discuss amendment 117 and explain why we want to remove it. If the regulation is to remain, it is vital that the Competition and Markets Authority be consulted before regulations are made due to the impact they will likely have in entrenching power in the hands of browser owners. That the Government have recognised that it was an oversight not to involve the CMA in any consultations is really pleasing. I offer my full support to the amendment in that context, though I do not believe it goes far enough and will advocate the removal of regulation 6B entirely in due course.

Amendment 49 agreed to.

Amendments made: 50, in clause 79, page 102, line 25, leave out "disable or".

Clause 79 amends regulation 6 of the PEC Regulations to create new exceptions from the prohibition on storing and accessing information in terminal equipment. New paragraph (2C) contains an exception for software updates that satisfy specified requirements. This amendment removes a requirement for subscribers and users to be able to disable, not just postpone, the update.

Amendment 51, in clause 79, page 102, leave out lines 27 to 29.

Clause 79 amends regulation 6 of the PEC Regulations to create new exceptions from the prohibition on storing and accessing information in terminal equipment. New paragraph (2C) contains an exception for software updates that satisfy specified requirements. This amendment removes a requirement that, where the update takes effect, the subscriber or user can remove or disable the software.

Amendment 52, in clause 79, page 104, line 20, leave out "or supplementary provision" and insert

", supplementary, transitional, transitory or saving provision, including provision".—*(Sir John Whittingdale.)*

This amendment provides that regulations under the new regulation 6A of the PEC Regulations, inserted by clause 79, can include transitional, transitory or saving provision.

Stephanie Peacock: I beg to move amendment 117, in clause 79, page 104, line 32, leave out from the beginning to end of line 38 on page 105.

I begin by re-emphasising my overarching support for exploring ways to reduce consent fatigue and cookie banners. However, because of the direction that new regulation 6B takes us in, it requires far more consultation before entering the statute book. My amendment seeks to remove it. Regulation 6B aims, at some point in the future, to enable users to express any consent they wish to give or objections they wish to make regarding cookies to an operator of a website—commonly a browser—so that this can be done automatically on visiting the website. The three main concerns I have with this must be addressed and consulted on before such a regulation becomes law.

I am concerned that it will pose concerns for competition if browsers, often owned by powerful global tech companies, are given centralised control and access to data surrounding cookies across the entire internet. That concern was echoed by the Advertising Association and the CEO of the Data and Marketing Association during an oral evidence session. When asked whether there was any concern that centralising cookies by browser will entrench power in the hands of the larger tech companies that own the browsers, Chris Combemale answered:

"It certainly would give even greater market control to those companies."—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 21, Q43.]

He said:

"If anything, we need more control in the hands of the people who invest in creating the content"—[Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee, 10 May 2023; c. 21, Q42.]

online.

9.45 am

Secondly, browser-enabled models could confuse liability and damage website direct relationships with customers. Indeed, any system of this kind would inevitably require browsers to be able to interrupt a provider's relationship with their customers by automatically overriding the consent directly expressed to them by their users. That would make confusing who is liable if data is processed in a way the data subject would like to dispute. The relationship is not only relevant when things go wrong. In general, media owners should be able to develop first-party relationships with their audiences and customers to better understand what they need without having browsers as gatekeepers of the information.

Many, including techUK, have questioned the technological readiness of browser-based solutions. That was also highlighted in the responses to the Government's "Data: a new direction" consultation. Although regulation 6B recognises this by allowing for browser-enabled models to be implemented in the future rather than immediately, given the previous concerns highlighted it seems reasonable to expect that proper parliamentary scrutiny will be required at the point where we actually know what the technology looks like. For those reasons, as a collective we must oppose the inclusion of regulation 6B. This is not to say that a similar model, with proper consultation and scrutiny, may not at some point come to fruition and work well, but at this point in time further review is needed before the option to enact browser-enabled models is on the statute book.

Sir John Whittingdale: As the hon. Lady sets out, amendment 117 would remove new regulation 6B from the Bill, but we see this as an important tool for reducing frequent cookie consent banners and pop-ups that can, as we have debated already, interfere with people's use of the internet. Members will be aware, as has already been set out, that clause 79 removes the need for organisations to seek consent to place cookies for certain non-intrusive purposes. One way of further reducing the need for repeated cookie pop-up notices is by blocking them at source—in other words, allowing web users to select which cookies they are willing to accept and which they are not comfortable with by using browser-level settings or similar technologies. These technologies should allow users to set their online preferences once and be confident that those choices will be respected throughout their use of the internet.

We will continue to work with the industry and the Information Commissioner to improve take-up and effectiveness of browser-based and similar solutions. Retaining the regulation-making powers at 6B is important to this work because it will allow the Secretary of State to require relevant technologies to meet certain standards or specifications.

Without regulations, there could be an increased risk of companies developing technologies that did not give web users sufficient choice and control about the types of cookies they are willing to accept. We will consult widely before making any new regulations under 6B, and new regulations will be subject to the affirmative resolution procedure. We have listened to stakeholders and intend to amend 6B to provide an explicit requirement for the Secretary of State to consult the Competition and Markets Authority before making new regulations.

Damian Collins (Folkestone and Hythe) (Con): Is this something the Department has considered? For example, Google Chrome has a 77% share of the web browser market on desktop computers, and over 60% for all devices including mobile devices. Although we want to improve the use of the internet for users and get rid of unwanted cookies, the consequence would be the consolidation of power in the hands of one or two companies with all that data.

Sir John Whittingdale: I entirely agree with my hon. Friend. He accurately sums up the reason that the Government decided it was important that the Competition and Markets Authority would have an input into the development of any facility to allow browser users to set their preferences at the browser level. We will see whether, with the advent of other browsers, AI-generated search engines and so on, the dominance is maintained, but I think he is absolutely right that this will remain an issue that the Competition and Markets Authority needs to keep under review.

That is the purpose of Government amendment 54, which will ensure that any competition impacts are considered properly. For example, we want any review of regulations to be relevant and fair to both smaller

[Sir John Whittingdale]

publishers and big tech. On that basis, I hope that the hon. Member for Barnsley East will consider withdrawing her amendment.

Stephanie Peacock: I appreciate the Minister's comments and the Government change involving the CMA, but we simply do not believe that that is worth putting into law. We just do not know the full implications, as echoed by the hon. Member for Folkestone and Hythe. I will therefore press my amendment to a Division.

Question put, That the amendment be made.

The Committee divided: Ayes 4, Noes 8.

Division No. 26]

AYES

Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

Question accordingly negatived.

Amendments made: 53, in clause 79, page 105, line 11, after "transitional" insert ", transitory".

This amendment makes clear that regulations under the new regulation 6B of the PEC Regulations, inserted by clause 79, can include transitory provision.

Amendment 54, in clause 79, page 105, line 15, at end insert—

"(aa) the Competition and Markets Authority, and".—*(Sir John Whittingdale.)*

This amendment requires the Secretary of State to consult the Competition and Markets Authority before making regulations under regulation 6B of the PEC Regulations.

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

Sir John Whittingdale: I shall not repeat all that has been said about the purpose of the clause. To recap quickly, consent is required for any non-essential functions, such as audience measurement, design optimisation, presentation of adverts and tracking across websites but, clearly, the current system is not working well. Researchers found that people often click yes to cookies to make the banner go away and because they want to access the service quickly.

The clause will remove the requirement for organisations to seek consent to cookies placed for several low privacy risk purposes. As a result of the new exceptions we are introducing, web users should know that if they continue to see cookie pop-up messages it is because they relate to more intrusive uses of cookies. It is possible that we may identify additional types of non-intrusive cookies in the future, so the clause permits the Secretary of State to make regulations amending the exceptions to the consent requirement or introducing new exceptions.

The changes will not completely remove the existence of cookie pop-ups. However, we are committed to working with tech companies and consumer groups to promote technologies that help people to set their online preferences at browser level or by using apps. Such technology has the potential to reduce further the number of pop-ups that appear on websites. Alongside the Bill, we will take forward work to discuss what can be done further to develop and raise awareness of possible technological solutions. On that basis, I commend the clause to the Committee.

Stephanie Peacock: I spoke in detail about my issues with the clause during our debates on amendments 116 and 117, but overall I commend the Government's intention to explore ways to end cookie fatigue. Although I unfortunately do not believe that these changes will solve the issues, it is pleasing that the Government are looking at ways to reduce the need for consent where the risk for privacy is low. I will therefore not stand in the way of the clause, beyond voicing my opposition to regulation 6B.

Question put and agreed to.

Clause 79, as amended, accordingly ordered to stand part of the Bill.

Clause 80

UNRECEIVED COMMUNICATIONS

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

The Chair: With this it will be convenient to discuss clauses 81 and 82 stand part.

Sir John Whittingdale: Clause 80 provides an additional power for the Information Commissioner when investigating unsolicited direct marketing through telephone calls, texts and emails—more commonly known as nuisance calls or nuisance communications.

Some unscrupulous direct marketing companies generate hundreds of thousands of calls to consumers who have not consented to be contacted. That can affect the most vulnerable in our society, some of whom may agree to buy products or services that they did not want or cannot afford. Successive Governments have taken a range of actions over the years—for example, by banning unsolicited calls from claims management firms and pensions providers—but the problem persists and further action is needed.

Under the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Information Commissioner can investigate and take enforcement action against rogue companies where there is evidence that unsolicited marketing communications have been received by the recipient. The changes we are making in clause 80 will enable the Information Commissioner to take action in relation to unsolicited marketing communications that have been generated, as well as those received or connected.

Not every call that is generated reaches its intended target. For example, an individual may be out or may simply not pick up the phone. However, the potential for harm should be a relevant factor in any enforcement action by the Information Commissioner's Office. The

application of the regulations, through the changes in clause 80, to communications generated will more accurately reflect the level of intent to cause disturbance.

Clause 81 is a minor and technical clause that should improve the readability of the PEC regulations. The definition of "direct marketing", which the PEC regulations rely on, is currently found in the Data Protection Act 1998. To help the reader quickly locate the definition, the clause adds the definition to the PEC regulations themselves.

Under the current PEC regulations, businesses can already send direct marketing to existing customers, subject to certain safeguards. That is sometimes known as the soft opt-in rule. Clause 82 applies the same rule to non-commercial organisations, such as charities. The changes will mean that charitable, political and non-commercial organisations will be able to send direct marketing communications to persons who have previously expressed an interest in the organisation's aims and ideals.

The current soft opt-in rules for business are subject to certain safeguards. We have applied the same safeguards to these new provisions for non-commercial organisations. We think these changes will help non-commercial organisations, including charities and political parties, to build ongoing relationships with their supporters. There is no good reason why the soft opt-in rule should apply to businesses but not to non-commercial organisations. I hope Members will see the benefit of these measures in ensuring the balance between protecting the most vulnerable in society and supporting organisations. I commend clauses 80 to 82 to the Committee.

Stephanie Peacock: As I have said many times during our discussion of the Bill, I believe that the Information Commissioner should be given proportionate powers to investigate and take action where that is needed to uphold our regulations. That is no less the case with clause 80, which introduces measures that allow the Information Commissioner to investigate organisations responsible for generating unsolicited direct marketing communications, even if they are not received by anyone.

Clause 81 simply lifts the definition of "direct marketing" from the Data Protection Act 1998 and places it into the PEC regulations to increase the readability of that legislation. I have no issues with that.

Clause 82 extends the soft opt-in rules to charities and non-commercial organisations. It is only right that the legislation is consistent in offering non-profits the opportunity to send electronic marketing communications in the same way as for-profit organisations. It might, however, be worth raising the public's awareness of the rule and of the ability to opt out at any point. If they suddenly find themselves on the end of such communications, they will have a clear understanding of why that is the case and that consent may be withdrawn if they so wish.

Question put and agreed to.

Clause 80 accordingly ordered to stand part of the Bill.

Clauses 81 and 82 ordered to stand part of the Bill.

Clause 83

DIRECT MARKETING FOR THE PURPOSES OF DEMOCRATIC ENGAGEMENT

10 am

Sir John Whittingdale (Maldon) (Con): I beg to move amendment 55 in clause 83, page 107, line 41, leave out 'or transitional' and insert ', transitional, transitory or saving'.

This amendment provides that regulations under clause 83 can make transitory or saving provision.

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

Clauses 83 and 84 stand part.

Sir John Whittingdale: Before I speak to the amendment, I will set out the provisions of clause 83, which gives the Secretary of State the power to make exceptions to the PEC regulations' direct marketing provisions for communications sent for the purposes of democratic engagement. We do not intend to use the powers immediately because the Bill contains a range of other measures that will facilitate a responsible use of personal data for the purposes of political campaigning, including the extension of the soft opt-in rule that we have just debated. However, it is important we keep the changes we are making in the Bill under review to make sure that elected representatives and parties can continue to engage transparently with the electorate and are not unnecessarily constrained by data protection and privacy rules.

The Committee will note that if the Secretary of State decided to exercise the powers, there are a number of safeguards in the clause that will maintain a sensible balance between the need for healthy interaction with the electorate and any expectations that an individual might have with regard to privacy rights. Any new exceptions would be limited to communications sent by the individuals and organisations listed in clause 83, including elected representatives, registered political parties and permitted participants in referendum campaigns.

Before laying any regulations under the clause, the Secretary of State will need to consult the Information Commissioner and other interested parties, and have specific regard for the effect that further exceptions could have on the privacy of individuals. Regulations will require parliamentary approval via the affirmative resolution procedure. Committee members should also bear in mind that the powers will not affect an individual's right under the UK GDPR to opt out of receiving communications.

We have also tabled two technical amendments to the clause to improve the way it is drafted. Government amendment 55 will make it clear that regulations made under this power can include transitory or savings provisions in addition to transitional provisions. Such provisions might be necessary if, for example, new exceptions were only to apply for a time-limited period. Clause 84 is also technical in nature and simply sets out the meaning of terms such as "candidate", "elected representative" and "permitted participant" for the purposes of clause 83.

Stephanie Peacock: The clauses mirror somewhat the involvement of democratic engagement purposes on the recognised legitimate interests list. However, here, rather than giving elected representatives and the like

[Stephanie Peacock]

an exemption from completing a balancing test when processing under this purpose, the Bill paves the way for them to be exempt from certain direct marketing provisions in future.

The specific content of any future changes, however, should be properly scrutinised. As such, it is disappointing that the Government have not indicated how they intend to use such regulations in future. I appreciate that the Minister has just said that they do not intend to use them right now. Does he have in mind any examples of any exemptions that he might like to make from the direct marketing provisions for democratic engagement purposes? That is not to say that such exemptions will not be justified; just that their substance should be openly discussed and democratically scrutinised.

Sir John Whittingdale: As I have set out, the existing data protection provisions remain under the GDPR. In terms of specific exemptions, I have said that the list will be subject to future regulation making, which will be also subject to parliamentary scrutiny. We will be happy to supply a letter to the hon. Lady to set out specific examples of where that might be the case.

Amendment 55 agreed to.

Clause 83, as amended, ordered to stand part of the Bill.

Clause 84

MEANING OF EXPRESSIONS IN SECTION 83

Amendment made: 31, in clause 84, page 110, line 31, leave out "fourth day after" and insert

"period of 30 days beginning with the day after".—*(Sir John Whittingdale.)*

Clauses 83 and 84 enable regulations to make exceptions from direct marketing rules in the PEC Regulations, including for certain processing by elected representatives. This amendment increases the period for which former members of the Westminster Parliament and the devolved legislatures continue to be treated as "elected representatives" following an election. See also NC6 and Amendment 30.

Clause 84, as amended, ordered to stand part of the Bill.

Clause 85

DUTY TO NOTIFY THE COMMISSIONER OF UNLAWFUL DIRECT MARKETING

Sir John Whittingdale: I beg to move amendment 56, in clause 85, page 112, line 35, at end insert—

"(13A) Regulations under paragraph (13) may make transitional provision.

(13B) Before making regulations under paragraph (13), the Secretary of State must consult—

(a) the Commissioner, and

(b) such other persons as the Secretary of State considers appropriate."

This amendment enables regulations changing the amount of a fixed penalty under regulation 26B of the PEC Regulations to include transitional provision. It also requires the Secretary of State to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate before making such regulations.

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

Amendment 118, in clause 85, page 113, line 3, at end insert—

"(1A) Guidance under this section must—

(a) make clear that a provider of a public electronic communications service is not obligated to monitor the content of individual electronic communications in order to determine whether those communications contravene the direct marketing regulations; and

(b) include illustrative examples of the grounds on which a provider may reasonably suspect that a person is contravening or has contravened any of the direct marketing regulations."

Government amendment 33.

Clause stand part.

Sir John Whittingdale: Before I speak to Government amendment 56, it might be helpful to set out the provisions of clause 85. The clause will help to ensure that there is better co-operation between the industry and the regulator in tackling the problem of nuisance communications. It places a duty on public electronic communications service and network providers to notify the Information Commissioner within 28 days if they have "reasonable grounds" for suspecting that unlawful direct marketing communications are transiting their services or networks. Once notified, the ICO will investigate whether a breach of the PEC regulations has occurred and take appropriate action where necessary.

We cannot expect network and service providers to know for certain whether a customer has agreed to receive a marketing call, which is why the new requirement is predicated on the organisation having reasonable grounds for suspecting that something unlawful is occurring. For example, there might be cases where a communications network or service provider notices a large volume of calls being generated in quick succession, with only one digit in the telephone number changing each time. That might suggest that calls are being made indiscriminately, without regard to whether the customer has registered with the telephone preference service or previously advised the caller that they did not want to be contacted.

We do not envisage that the provision will place significant new burdens on the network and service providers. It does not require them to put new systems in place to monitor for suspicious activities. However, where they have that capability already and have reasonable grounds to believe that unlawful activity is going on, we would like them to share that information with the ICO. The clause also requires the ICO to produce and publish guidance for network and service providers to help them to understand what intelligence information could reasonably be shared.

I shall respond to amendment 118 after the hon. Member for Barnsley East has spoken to it, but it might be helpful for me briefly to explain Government amendment 56. The fixed penalty for failure to comply with the duty, which is currently set at £1,000, is being kept under review. Where appropriate, the Secretary of State can use regulations to change the fine amount. The amendment will ensure that those regulation-making powers are consistent with similar powers elsewhere in the Bill. The regulations could include transitional provisions, and the amendment will also require the

Secretary of State to consult the Information Commissioner and other persons they consider appropriate before making such regulations.

Government amendment 33 is a minor and technical change designed to improve the readability of the legislation.

The Chair: The amount is fixed in the Bill at £1,000, Minister. That is stated at clause 85 in proposed new regulation 26B. The Bill states:

"The amount of a fixed monetary penalty under this regulation shall be £1,000."

That does not indicate any flexibility. I draw that to the attention of the Committee.

Sir John Whittingdale: But, as I have set out, that is subject to review.

The Chair: Thank you.

Stephanie Peacock: The ambition of the clause is broadly welcome, and we agree that there is a need to tackle unwanted calls, but the communications sector, including Vodafone and BT, as well as techUK, has shared concerns that the clause, which will place a new duty on telecoms providers to report to the commissioner whenever they have "reasonable grounds" for suspecting a breach of direct marketing regulations, might not be the best way to solve the issue.

I will focus my remarks on highlighting those concerns, and how amendment 118 would address some of them. First, though, let me say that the Government have already made it clear in their explanatory notes that it is not the intention of the Bill to require providers to monitor communications. However, that has not been included in the Bill, which has caused some confusion in the communications sector.

Amendment 118 would put that confusion to rest by providing for the explicit inclusion of the clarification in the clause itself. That would provide assurances to customers who would be sure their calls and texts would not be monitored, and to telecoms companies, which would be certain that such monitoring of content was absolutely not required of them.

Secondly, the intent of the clause is indeed not to have companies monitoring communications, but many relevant companies have raised concerns around the technological feasibility of identifying instances of unlawful and unsolicited direct marketing. Indeed, the new duty will require telecommunications providers to be able to identify whether a person receiving a direct marketing call has or has not given consent to receive the call from the company making it. However, providers have said they cannot reliably know that, and have warned that there is no existing technology to conduct that kind of monitoring accurately and at scale. In the absence of communication monitoring and examples of how unsolicited direct marketing is to be identified, it is therefore unclear how companies will fulfil their duties under the clause.

That is not to say the industry is not prepared to commit significant resources to tackling unwanted calls. BT, for example, has set up a range of successful tools to help customers. That includes BT Call Protect, which is used by 4.4 million BT customers and now averages 2.35 million calls diverted per week. However, new measures must be feasible, and our amendment 118 would therefore require that guidance around the implementation of the clause include illustrative examples of the grounds on which a provider may reasonably suspect that a person is contravening, or has contravened, any of the direct marketing regulations.

If the Minister does not intend to support the amendment, I would like to hear such examples from him today, so that the communications sector was absolutely clear about how to fulfil its new duties, given the technology available.

Sir John Whittingdale: As the hon. Lady has said, amendment 118 would require the commissioner to state clearly in the guidance that the new duty does not oblige providers to intercept or monitor the content of electronic communications in order to determine whether there has been a contravention of the rules. It would also require the guidance to include illustrative examples of the types of activity that may cause a provider reasonably to suspect that there had been a contravention of the requirements.

I recognise that the amendment echoes concerns that have been raised by communications service providers, and that there has been some apprehension about exactly what companies will have to do to comply with the duty. In response, I would emphasise that "reasonable grounds" does mean reasonable in all circumstances.

The hon. Lady has asked for an example of the kind of activity that might give reasonable grounds for suspicion. I direct her to the remarks I made in moving the amendment and the example of a very large number of calls being generated in rapid succession in which, in each case, the telephone number is simply one digit away from the number before. The speed at which that takes place does provide reasonable grounds to suspect that the requirement to, for instance, check with the TPS is not being fulfilled.

There are simple examples of that kind, but I draw the attention of the hon. Lady and the Committee to the consultation requirements that will apply to the ICO's guidance. In addition to consulting providers of public electronic communications networks and services on the development of the guidance, the ICO will be required to consult the Secretary of State, Ofcom and other relevant stakeholders to ensure that the guidance is as practical and useful to organisations as possible.

10.15 am

Damian Collins: Does my right hon. Friend agree that, if amendment 118 were made, it could be used as a general get-out-of-jail-free card by companies? Let us consider, for example, a situation where a company could easily and obviously have spotted a likely breach of the regulations and should have intervened. When the commissioner discovered that the company had failed in its duty to do so, the company could turn around and say, "Well, yes, we missed that, but we were not under any obligation to monitor." It is therefore important that there is a requirement for companies to use their best endeavours to monitor where possible.

Sir John Whittingdale: I completely agree; my hon. Friend is right to make that distinction. Companies should use their best endeavours, but it is worth repeating

[Sir John Whittingdale]

that the guidance does not expect service and network providers to monitor the content of individual calls and messages to comply with the duty. There is more interest in patterns of activity on networks, such as where a rogue direct marketing firm behaves in the manner that I set out. On that basis, I ask the hon. Lady not to press her amendment to a vote.

Stephanie Peacock: I appreciate the Minister's comments and those of the hon. Member for Folkestone and Hythe. We have no issue with the monitoring of patterns; we wanted clarification on the content. I am not sure that the Minister addressed the concerns about the fact that, although the Government have provided a partial clarification in the explanatory notes, this is not in the Bill. For that reason, I will press my amendment to a vote.

Amendment 56 agreed to.

Amendment proposed: 118, in clause 85, page 113, line 3, at end insert—

"(1A) Guidance under this section must—

(a) make clear that a provider of a public electronic communications service is not obligated to monitor the content of individual electronic communications in order to determine whether those communications contravene the direct marketing regulations; and

(b) include illustrative examples of the grounds on which a provider may reasonably suspect that a person is contravening or has contravened any of the direct marketing regulations."—*(Stephanie Peacock.)*

Question put, That the amendment be made.

The Committee divided: Ayes 4, Noes 8.

Division No. 27]

AYES

Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John

Question accordingly negatived.

Amendment made: 33, in clause 85, page 113, line 28, at end insert—

"(4) After regulation 18 insert—

'Direct marketing

(1) Regulations 19 to 26C make provision about direct marketing.

(2) See also section 83 of the Data Protection and Digital Information Act 2023 (which provides for regulations to make exceptions to regulations 19 to 24).'"—*(Sir John Whittingdale.)*

This amendment inserts into the PEC Regulations provision introducing the regulations dealing with direct marketing (including regulations amended or inserted by the Bill) and cross-referring to the regulation-making power in clause 83 of the Bill.

Clause 85, as amended, ordered to stand part of the Bill.

Clause 86

DUTY TO NOTIFY THE COMMISSIONER OF UNLAWFUL DIRECT MARKETING

Sir John Whittingdale: I beg to move amendment 57, in clause 86, page 113, line 38, at end insert—

"(13A) Regulations under paragraph (13) may make transitional provision.

(13B) Before making regulations under paragraph (13), the Secretary of State must consult—

(a) the Information Commissioner, and

(b) such other persons as the Secretary of State considers appropriate."

This amendment enables regulations changing the amount of a fixed penalty under regulation 5C of the PEC Regulations to include transitional provision. It also requires the Secretary of State to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate before making such regulations.

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

Clause stand part.

Government amendments 32 and 58.

That schedule 10 be the Tenth schedule to the Bill.

Sir John Whittingdale: Before turning specifically to the provisions of the amendment, I will set out the provisions of clause 86 and schedule 10. Clause 86 updates the ICO's powers in respect of enforcing the PEC regulations. Currently, the ICO has to rely mainly on outdated powers in the Data Protection Act 1998 to enforce breaches of the PEC regulations. The powers were not updated when the UK GDPR and the Data Protection Act came into force in 2018. That means that some relatively serious breaches of the PEC regulations, such as nuisance calls being generated on an industrial scale, cannot be investigated as effectively or punished as severely as breaches under the data protection legislation.

The clause will therefore give the ICO the same investigatory and enforcement powers in relation to breaches of the PEC regulations as currently apply to breaches of the UK GDPR and the 2018 Act. That will result in a legal framework that is more consistent and predictable for organisations, particularly for those with processing activities that engage both the PEC regulations and the UK GDPR.

Clause 86 and schedule 10 add a new schedule to the PEC regulations, which sets out how the investigatory and enforcement powers in the 2018 Act will be applied to the PEC regulations. Among other things, that includes the power for the Information Commissioner to impose information notices, assessment notices, interview notices and enforcement and penalty notices. The maximum penalty that the Information Commissioner can impose for the most serious breaches of the PEC regulations will be increased to the same levels that can be imposed under the UK GDPR and the Data Protection Act. That is up to 4% of a company's annual turnover or £17.5 million, whichever is higher.

Relevant criminal offences under the Data Protection Act, such as the offence of deliberately frustrating an investigation by the Information Commissioner by destroying or falsifying information, are also applied to the PEC regulations. The updated enforcement provisions

in new schedule 1 to the PEC regulations will retain some pre-existing powers that are unique to the previous regulations.

Clause 86 also updates regulation 5C of the PEC regulations, which sets out the fixed penalty amount for a failure to report a personal data breach under regulation 5. Currently, the fine level is set at £1,000. The clause introduces a regulation-making power, which will be subject to the affirmative procedure, for the Secretary of State to increase the fine level. We have tabled Government amendment 57 to provide an explicit requirement for the Secretary of State to consult the Information Commissioner and any other persons the Secretary of State considers appropriate before making new regulations. The amendment also confirms that regulations made under the power can include transitional provisions.

Finally, we have tabled two further minor amendments to schedule 10. Government amendment 58 makes a minor correction by inserting a missing schedule number. Government amendment 32 adjusts the provision that applies section 155(3)(c) of the Data Protection Act for the purposes of the PEC regulations. That is necessary as that section is being amended by schedule 4. Without making those corrective amendments, the provisions will not achieve the intended effect.

Stephanie Peacock: Clause 86 and schedule 10 insert and clarify the commissioner's enforcement powers with regards to privacy and electronic communications regulation. Particularly of note within the proposals is the move to increase fines for nuisance calls and messages to a higher maximum penalty of £17.5 million or 4% of the undertaking's total annual worldwide turnover, whichever is higher. That is one of the Government's headline commitments in the Bill and should create tougher punishments for those who are unlawfully pestering people through their phones.

We are in complete agreement that more must be done to stop unwanted communications. However, to solve the problem as a whole, we must take stronger action on scam calling as well as on instances of unsolicited direct marketing. Labour has committed to going further than Ofcom's new controls on overseas scam calls and has proposed the following to close loopholes: first, no phone call made from overseas using a UK telephone number should have that number displayed when it appears on a UK mobile phone or digital landline; and secondly, all mobile calls from overseas using a UK number should be blocked unless the network provider confirms that the known bill payer for the number is currently roaming. To mitigate the fact that some legitimate industries rely on overseas call centres that handle genuine customer service requests, we will also require Ofcom to register those legitimate companies and their numbers as exceptions to the blocking.

As the clause and schedule seek to take strong action against unwanted communications, I would be pleased to hear from the Minister whether the Government would consider going further and matching our commitments on overseas scam calling, too.

Sir John Whittingdale: I say to the hon. Lady that the provisions deal specifically with nuisance calls, not necessarily scam calls. As she will know, the Government have a comprehensive set of policies designed to address fraud committed through malicious or scam calls, and those are being processed through the fraud prevention strategy. I accept that more needs to be done and say to her that it is already taking place.

Amendment 57 agreed to.

Clause 86, as amended, ordered to stand part of the Bill.

Schedule 10

PRIVACY AND ELECTRONIC COMMUNICATIONS: COMMISSIONER'S ENFORCEMENT POWERS

Amendments made: 32, in schedule 10, page 180, line 25, leave out "for "data subjects"" and insert

"for the words from "data subjects" to the end".

This amendment adjusts provision applying section 155(3)(c) of the Data Protection Act 2018 (penalty notices) for the purposes of the PEC Regulations to take account of the amendment of section 155(3)(c) by Schedule 4 to the Bill.

Amendment 58, in schedule 10, page 183, line 5, at end insert "15".—*(John Whittingdale.)*

This amendment inserts a missing Schedule number, so that the provision refers to Schedule 15 to the Data Protection Act 2018.

Schedule 10, as amended, agreed to.

Clause 87

THE EIDAS REGULATION

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

The Chair: With this it will be convenient to discuss clauses 88 to 91 stand part.

Sir John Whittingdale: Clauses 87 to 91 make changes to the UK's eIDAS regulation to support the effective functioning of the UK's trust services market into the future. Clause 87 states that when clauses 88 to 91 talk about the eIDAS regulation, this refers to regulation 910/2014, on electronic identification and trust services for electronic transactions in the internal market, which was adopted by the European Parliament and the European Council on 23 July 2014.

There is potential for confusion between the UK eIDAS regulation and the EU eIDAS regulation from which it stems and which shares the same title. I can confirm that all references to the eIDAS regulation in clauses 88 to 91 refer to the regulation as it was retained and modified on EU exit to apply within the UK.

Clause 88 amends the UK eIDAS regulation so that conformity assessment reports issued by an accredited EU conformity assessment body can be recognised and used to grant a trust service provider qualified status under the regulation. UK-qualified trust services are no longer legally recognised within the EU, which has meant that qualified trust service providers who wish to operate within both the UK and the EU need to meet two sets of auditing requirements. That is not cost effective and creates regulatory barriers in the nascent UK trust services market. Unilateral recognition of EU conformity assessment bodies will remove an unnecessary regulatory barrier for qualified trust service providers wishing to operate within both the UK and EU markets.

[Sir John Whittingdale]

Clause 89 provides the Secretary of State with a power to revoke articles 24A and 24B of the UK eIDAS regulation in the future, should the continued unilateral recognition of EU-qualified trust services, and the recognition of conformity assessment reports issued by EU conformity assessment bodies, no longer meet the needs of the UK market. Clause 89 also provides a power to amend article 24A in order to wind down the recognition of EU-qualified trust services, by removing the recognition of certain elements of EU-qualified trust service standards only.

For example, it will be possible to continue to recognise EU-qualified electronic time stamps and delivery services while ending the recognition of EU-qualified electronic signatures and seals, which will give the UK eIDAS regulation flexibility to adapt to future changes. The clause provides that any regulations made under this power will be subject to the negative resolution procedure.

10.30 am

Clause 90 inserts articles 45A, 45B and 45C into the UK eIDAS regulation, providing the Secretary of State with powers to make regulations to recognise and give legal effect to trust service products provided by entities established outside the UK, on the basis of equivalent reliability to comparable UK trust service products. The legal effect of overseas trust service products, which are specified within regulations made under article 45A, will be equivalent to the legal effect of qualified trust service products provided by a qualified trust service provider established in the United Kingdom.

Two conditions apply when making regulations under article 45A. First, the Secretary of State must be satisfied that the reliability of an overseas trust service product is at least equivalent to the reliability of its qualified counterpart under the eIDAS regulation. Secondly, he must have regard to the relevant overseas law concerning the type of trust service product to be recognised.

The clause provides that the Secretary of State must consult the Information Commissioner, as the UK supervisory body for trust services, before making regulations, and that any regulations made under article 45A or 45B will be subject to the negative resolution procedure. We believe that the measure will help ensure that the UK is well placed to agree mutual recognition of trust service products with other countries to boost the growth in cross-border electronic transactions.

Clause 91 provides a power for the Secretary of State within regulations to designate overseas trust service regulatory authorities, which the Information Commissioner, as the supervisory body for UK trust services, may give information and assistance to and co-operate with in the interests of effective regulation of trust services. That measure will help to future-proof the UK trust services framework, so it can better support the growing demand for secure and trusted electronic transactions across the global digital economy. It provides that the Secretary of State must consult the Information Commissioner before making regulations under this power. It also provides that any regulations made under this power will be subject to the negative resolution procedure.

I hope that Members will recognise the merits of that approach. As the digital economy grows and the demand for UK-based qualified trust service providers is rising, these clauses will ensure that the UK's trust services framework is future-proofed and able to support the growing demand for trusted digital transactions globally.

Stephanie Peacock: "Trust services" refers to services including those relating to electronic signatures, electronic seals, timestamps, electronic delivery services and website authentication. As has been mentioned, trust services are required to meet certain standards and technical specifications for operation across the UK economy, which are outlined under eIDAS regulations. These clauses seek to make logistical adjustments to that legal framework for trust service products and services within in the UK.

Although we understand that the changes are intended to enable flexibility in case EU regulations should no longer be adequate, and absolutely agree that we must future-proof regulations to ensure that standards are always kept high, we must also ensure that any changes made are necessary, to ensure that standards remain high, rather than being made simply for their own sake. It is vital that any alterations made are genuinely intended to improve current practices and have been thoroughly considered to ensure that they are making positive and meaningful change.

Question put and agreed to.

Clause 87 accordingly ordered to stand part of the Bill.

Clauses 88 to 91 ordered to stand part of the Bill.

Clause 92

DISCLOSURE OF INFORMATION TO IMPROVE PUBLIC SERVICE DELIVERY TO UNDERTAKINGS

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

Sir John Whittingdale: The clause will amend the Digital Economy Act 2017 to extend the powers under section 35 to include businesses. Existing powers enable public authorities to share data to support better services to individuals and households. The Government believe that businesses too can benefit from responsive, joined-up public services across the digital economy. The clause introduces new data sharing powers allowing specified public authorities to share data with other specified public authorities for the purposes of fulfilling their functions.

The sharing of data will also provide benefits for the public in a number of ways. It will pave the way for businesses to access Government services more conveniently, efficiently and securely—by using digital verification services, accessing support when trying to start up new businesses, completing import and export processes or applying for Government grants such as rural grants, for example. Any data sharing will of course be carried out in accordance with the requirements of the Data Protection Act and the UK GDPR.

Being able to share data about businesses will bring many benefits. For example, by improving productivity while keeping employment high we can earn more, raising living standards, providing funds to support our public services and improving the quality of life for all citizens. Now that we have left the EU, businesses that take action to improve their productivity will increase

their resilience to changing market conditions and be more globally competitive. The Minister will be able to make regulations to add new public authorities to those already listed in schedule 4 to the Digital Economy Act. However, any regulations would be made by the affirmative procedure, requiring the approval of both Houses. I commend the clause to the Committee.

Stephanie Peacock: The clause amends section 35 of the Digital Economy Act to enable specified public authorities to share information to improve the delivery of public services to businesses with other specified persons. That echoes the existing legal gateway that allows for the sharing of information on improving the delivery of public services to individuals and households.

I believe that the clause is a sensible extension, but would have preferred the Minister and his Department to have considered public service delivery more broadly when drafting the Bill. While attention has rightly been paid throughout the Bill to making data protection regulation work in the interests of businesses, far less attention has gone towards how we can harness data for the public good and use it to the benefit of our public services. That is a real missed opportunity, which Labour would certainly have taken.

Question put and agreed to.

Clause 92 accordingly ordered to stand part of the Bill.

Clause 93

Implementation of law enforcement information-sharing agreements

Sir John Whittingdale: I beg to move amendment 8, in clause 93, page 119, line 18, leave out first "Secretary of State" and insert "appropriate national authority".

This amendment, Amendment 10 and NC5 enable the regulation-making power conferred by clause 93 to be exercised concurrently by the Secretary of State and, in relation to devolved matters, by Scottish Ministers and Welsh Ministers.

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

Government amendments 9 to 16.

Government new clause 5—*Meaning of "appropriate national authority".*

Sir John Whittingdale: Clause 93 creates a delegated power for the Secretary of State, and a concurrent power for Welsh and Scottish Ministers, to make regulations to implement international agreements relating to the sharing of information for law enforcement purposes. The concurrent power for Welsh and Scottish Ministers has been included in an amendment to the clause. While international relations are a reserved matter, the domestic implementation of the provisions likely to be contained in future international agreements may be devolved, given that law enforcement is a devolved matter to various extents in each devolved Administration.

In the light of introducing a concurrent power for Welsh and Scottish Ministers, amendments to clauses 93 and 108 have been tabled, as has new clause 5. Together they specifically detail the appropriate national authority that will have the power to make regulations in respect of clause 93. The Government amendments make it clear that the appropriate national authority may make the regulations. New clause 5 then defines who is an appropriate national authority for those purposes. I therefore commend new clause 5 and the related Government amendments to the Committee.

Stephanie Peacock: It is right that the powers conferred by clause 93 can be exercised by devolved Ministers where appropriate. I therefore have no objections to the amendments or the new clause.

Amendment 8 agreed to.

Amendments made: 9, in clause 93, page 119, line 18, leave out second "Secretary of State" and insert "authority".

This amendment is consequential on Amendment 8.

Amendment 10, in clause 93, page 119, line 36, at end insert—

'"appropriate national authority" has the meaning given in section (Meaning of "appropriate national authority");'.—*(Sir John Whittingdale.)*

See the explanatory statement for Amendment 8.

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

Sir John Whittingdale: As I have already set out, clause 93 creates a delegated power for the Secretary of State, along with a concurrent power for Welsh and Scottish Ministers, to make regulations to implement international agreements relating to the sharing of information for law enforcement purposes. The legislation will provide powers to implement technical aspects of such international agreements via secondary legislation once the agreements have been negotiated.

Clause 93 stipulates that regulations can be made in connection with implementing an international agreement only in so far as it relates to the sharing of information for law enforcement purposes, and that any data sharing must comply with data protection legislation. These measures will enable the implementation of new international agreements designed to help keep the public safe from the threat posed by international criminality and cross-border crime, as well as helping to protect vulnerable people.

The Chair: I am assuming that Northern Ireland is covered by reserved matters.

Sir John Whittingdale: I believe the position is that at the present time, Northern Ireland does not have a functioning Assembly, so it is not possible, but that may change in due course.

The Chair: Hmm. Okay.

Stephanie Peacock: The clause allows the Secretary of State to make regulations to enact an international agreement for the sharing of information for law enforcement purposes. The substance of any such agreement will likely therefore come through secondary legislation and, as such, it will be appropriate at that point to scrutinise their contents. If the Minister and his Department have identified any targets for such agreements at this stage, I am sure that the Committee would be grateful to hear of them. If not, however, I expect that he would update the House of that through the usual channels.

Question put and agreed to.

Clause 93, as amended, accordingly ordered to stand part of the Bill.

Clause 94

FORM IN WHICH REGISTERS OF BIRTHS AND DEATHS ARE TO BE KEPT

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

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

Clauses 95 to 98 stand part.

That schedule 11 be the Eleventh schedule to the Bill.

Sir John Whittingdale: Clauses 94 to 98 amend the Registration Service Act 1953 and the Births and Deaths Registration Act 1953—which I will refer to as the Act—and introduce schedule 11, which contains minor and consequential amendments. Currently, under the Act, the Registrar General for England and Wales provides the local registration service with paper live birth, stillbirth and death registers and with paper forms for making certified copies of the register entries—for example, birth and death certificates. Since 2009, registrars in England and Wales also record birth and death registration information electronically, in parallel with the paper-based systems. That is a duplication of effort for registrars.

Clause 94(2) amends the Act and substitutes section 25 with a new section 25. The new section will allow the Registrar General to determine in which form registers of live births, stillbirths and deaths are to be kept, and contains additional provision appropriate for the keeping of registers in an electronic form only. New section 25(2) of the Act allows the Registrar General to require that registrars keep information in a form that will allow the Registrar General and the superintendent registrar to have immediate access to all live birth and death entries as soon as the registrar has entered the details in the register. In the case of stillbirths, new section 25(2)(b) allows the Registrar General to have immediate access to the entries in the register.

New section 25(3) provides that where a register is kept in such form as determined under new section 25(2)—for example, an electronic form—any information in that register made available to the Registrar General or superintendent registrar is deemed to be held by that person, as well as the registrar, when carrying out that person's functions—for example, the issue of certified copies.

Clause 94(3)(a) and (b) omit sections 26 and 27 of the Act, which set out the requirements for the quarterly returns made by a registrar and superintendent registrar. These returns will no longer be needed, as the superintendent registrar and the Registrar General will have immediate access to the records as provided for by new section 25 of the Act.

Clause 94(3)(c) omits section 28 of the Act, which sets out how paper registers must be stored by registrars, superintendent registrars and the Registrar General. With the introduction of new section 25, that provision is no longer necessary as it would not be relevant to an electronic register.

Proposed new section 25(4) of the Act provides that anything that is required for the purposes of creating and maintaining the registers—for example, providing registrars with the electronic system—is the responsibility of the Registrar General. Proposed new section 25(5) of the Act places a responsibility on the Registrar General to provide the required forms that the local registration service will need to produce certified copies of entries—for example, birth and death certificates.

10.45 am

Clause 95 inserts a new section 11A in the Registration Service Act 1953. That Act sets out the requirements for the appointment of registration officers by local authorities. Proposed new section 11A sets out that the council of every non-metropolitan county and metropolitan district, subject to the provisions of local scheme arrangements, must provide and maintain equipment or facilities that the Registrar General considers necessary for a superintendent registrar or registrar to carry out their functions—for example, the IT equipment needed to host an electronic register. It should be noted that IT equipment is already in place in register offices as births and deaths are currently recorded electronically in parallel with paper registers.

Currently, numerous sections of the Births and Deaths Registration Act 1953 require the paper registers to be signed by an informant when attending the register office to register a birth or death. The Act places a duty on the informant to provide the particulars required to be registered to a registrar and, in the presence of the registrar, to sign the register. Clause 96 makes provision for the signing, by the informant, of registers that are not kept in paper form, as we move towards digital methods of registering births and deaths and the introduction of an electronic register.

Clause 96(2) inserts a new section 38B—titled "Requirements to sign register"—into the Act 1953. That proposed new section empowers the Minister to make regulations regarding registers not kept in paper form. Proposed new section 38B(1)(a) provides that a duty to sign the register

"at any time is to have effect as a duty to comply with specified requirements",

while proposed new section 38B(3) clarifies that, in the section, "specified" means

"specified in regulations under this section".

Clause 96(3) states that regulations made by the Minister under proposed new section 38B are subject to the affirmative procedure. I reassure my hon. Friends that that will ensure full parliamentary oversight of the content of the regulations.

Clause 97 covers the treatment of the existing registers of births, stillbirths, deaths, and records. Clause 97(1)(a) specifies that the repeal of section 28 of the 1953 Act does not affect the existing requirement under section 28(2) for every superintendent registrar to continue to keep with the records of the office any registers of live births, or deaths, in their custody immediately before the repeal comes into force.

Clause 97(1)(b) specifies that the repeal of section 28 of the Act does not affect the existing requirement under section 28(4) for the Registrar General to continue to keep any certified copies that he has received under section 27 in the possession of the Registrar General and any registers of stillbirths forwarded to the Registrar General before the repeal coming into force.

Since 1 July 2009, birth and death records are held both in paper registers and in an electronic format. The Bill removes the requirement for birth and death entries to be held in paper format, removing the duplication in

process. Clause 97(5) specifies how copies of birth and death records that have been held in a format other than hard copy paper form, such as electronically, are to be treated on and after the day on which clause 94 of the Bill comes into force. Clause 97(6) outlines the period mentioned in clause 97(5) as beginning on 1 July 2009 and ending immediately before the day clause 94 comes into force.

Clause 98 introduces schedule 11, which contains minor and consequential amendments to primary legislation as a consequence of clauses 94 to 97. Part 1 of schedule 11 makes a number of amendments to the Births and Deaths Registration Act, and part 2 makes minor and consequential amendments to other primary legislation as a result of the changes brought about by the Bill.

Before sitting down, I pay tribute to my hon. Friend the Member for Solihull (Julian Knight), who attempted to introduce a number of these provisions via a private Member's Bill, which unfortunately did not make it through. His intention is now to be put into law as a result of the measures in this Bill.

Stephanie Peacock: Clauses 94 to 98 amend the Births and Deaths Registration Act, with the overall effect of removing the provision for birth and death records to be kept on paper, and allowing them to be held in an online database. This is a positive move, with the potential to bring many benefits. First, it will improve the functioning of the registration system—for example, it will allow the Registrar General and the superintendent registrar to have immediate access to all birth and death entries as soon as they have been entered into the system. The changes will undoubtedly be important to families who are experiencing joy or loss, because they make registrations easier and more likely to be correct in the first instance, minimising unnecessary clarifications at what can often be a very difficult time. Indeed, one of the recommendations of the 2022 UK Commission on Bereavement's landmark report, which looked at the key challenges facing bereaved people in this country, was that it should be possible to register deaths online.

It is great that the Government have chosen to pursue this change. However, despite it being the recommendation listed right next to online death registration, the Government have not used this opportunity to explore the potential of extending the Tell Us Once service, which is disappointing. Indeed, the existing Tell Us Once service has proved very helpful to bereaved people in reducing the administrative burden they face, by enabling them to inform a large number of Government and public sector bodies in one process, rather than forcing them to go through the same process time and again. However, private organisations are not included, and loved ones are still tasked with contacting organisations such as employers, energy and electricity companies, banks, telephone and internet providers, and more. At a time of emotional struggle, this is a huge administrative burden to place on the bereaved and leaves them vulnerable to other unsettling variables, such as communication barriers and potentially insensitive customer service.

The commission found that 61% of adult respondents reported experiencing practical challenges when notifying the organisations that need to be made aware of the death of a loved one. We are therefore disappointed that the Government have not explored whether the Bill could extend the policy to the private sector in order to further reduce the burden on grieving friends and families, and make the inevitably difficult process a little easier. Overall, however, the clauses will mark a positive change for families up and down the country, and we are pleased to see them implemented.

Sir John Whittingdale: I merely say to the hon. Lady that, having used the Tell Us Once service myself in relation to the death of my mother not that long ago, I absolutely hear what she says about the importance of making the process as easy as possible. We will certainly consider what she says.

Question put and agreed to.

Clause 94 accordingly ordered to stand part of the Bill.

The Chair: Congratulations to the hon. Member for Solihull.

Clauses 95 to 98 ordered to stand part of the Bill.

Schedule 11 agreed to.

Clause 99

INFORMATION STANDARDS FOR HEALTH AND ADULT SOCIAL CARE IN ENGLAND

Question proposed, That the clause stand part of the Bill

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

That schedule 12 be the Twelfth schedule to the Bill.

Sir John Whittingdale: Schedule 12 makes it clear that information standards published under section 250 of the Health and Social Care Act 2012, as amended by the Health and Care Act 2022, can include standards relating to information technology or IT services that are used or intended to be used in connection with the processing of information. The schedule extends the potential application of information standards to the providers of IT products and services to the health and adult social care sector for England. It also introduces mechanisms for monitoring and enforcing compliance by IT providers with information standards, and allows for the establishment of an accreditation scheme for IT products and services.

It is absolutely right that health and care information can flow in a standardised way between different IT systems and across organisational boundaries in the health and adult social care system in England, for the benefit of individuals and their healthcare outcomes. Information standards are vital to enabling that, alongside joint working between everyone involved in the processing of heath and care information.

These changes will support the efficient and effective operation of the health and adult social care system by making it easier for people delivering care to access accurate and complete information when they need it, improve clinical decision making and, ultimately, improve clinical outcomes for patients. The clause is a crucial enabler for the creation of a modern health and care service with systems that are integrated and responsive to the needs of patients and users. I therefore commend it to the Committee.

Stephanie Peacock: Information standards govern how data can be shared and compared across a sector. They are important in every sector in which they operate, but particularly in health, where they are critical to enabling the information sharing and interoperability necessary for good patient outcomes across health and social care services. For many reasons, however, we do not have a standard national approach to health data; as such, patients receive a far from seamless experience between different healthcare services. The Bill's technical amendments and clarifications of existing rules on information standards in health, and how they interact with IT and IT services, are small but good steps in the journey towards trying resolve that.

Tom Schumacher of Medtronic told us in oral evidence that one of the problems faced by his organisation and NHS trusts is

"variability in technical and IT security standards."

He suggested that harmonising those standards would be a "real opportunity," since it would mean that

"each trust does not have to decide for itself which international standard to use and which local standard to use."—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 42, Q90.]

However, it is unclear how much headway these IT-related changes will make in providing that harmonisation, let alone the seamless service that patients so often call for.

I have one query that I hope the Minister can help with. MedConfidential has shared with us a concern that new section 251ZE of the Health and Social Care Act 2012 on accreditation of information technology, which is introduced by schedule 12, seems to imply that the Department of Health and Social Care and NHS England will have the power to set data standards in social care. MedConfidential says that would be a major policy shift, and that it seems unusual to implement such a shift through an otherwise unrelated Bill. Will the Minister write to me to clarify whether it is the Government's intention to have DHSC and NHS England take over the information infrastructure of social care—and, if so, why they have come to that decision?

Sir John Whittingdale: I am grateful to the hon. Lady for her support in general. I hear the concern that she expressed on behalf of the firm that has been in contact with her. We will certainly look into that, and I will be happy to let her have a written response in due course.

Mr Paisley, might I beg the Committee's indulgence to correct the record? I incorrectly credited the hon. Member for Solihull for the private Member's Bill, but it was in fact my hon. Friend the Member for Meriden (Saqib Bhatti). I apologise to him for getting his constituency wrong—

The Chair: So we will take the congratulations away from Solihull and pass them elsewhere.

Sir John Whittingdale: I am afraid that congratulations have been removed from Solihull and transferred to Meriden.

The Chair: Better luck next time, Solihull! Thank you, Minister, for the correction.

Question put and agreed to.

Clause 99 accordingly ordered to stand part of the Bill.

Schedule 12 agreed to.

Ordered, That further consideration be now adjourned. —*(Steve Double.)*

10.59 am

Adjourned till this day at Two o'clock.

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Eighth Sitting

Tuesday 23 May 2023

(Afternoon)

CONTENTS

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 27 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
† Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Eastwood, Mark *(Dewsbury)* (Con)
† Henry, Darren *(Broxtowe)* (Con)
† Hunt, Jane *(Loughborough)* (Con)
Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Monaghan, Carol *(Glasgow North West)* (SNP)
Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
† Richards, Nicola *(West Bromwich East)* (Con)
Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 23 May 2023

(Afternoon)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

Clause 100

The Information Commission

2 pm

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

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

Government amendments 44 and 45.

That schedule 13 be the Thirteenth schedule to the Bill.

Clauses 101 to 103 stand part.

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): We now turn to part 5 of the Bill. Clauses 100 to 103 and schedule 13 will establish a body corporate, the Information Commission, to replace the existing regulator, the Information Commissioner, which is currently structured as a corporation sole. I should make it clear that the clauses will make no changes to the regulator's role and responsibilities; all the functions that rest with the Information Commissioner will continue to sit with the new Information Commission.

Clause 100 will establish a body corporate, the Information Commission, to replace the existing regulator, the Information Commissioner. The commission will be governed by an independent board, with chair and chief executive roles, thereby spreading the responsibilities of the Information Commissioner across a larger number of people.

Clause 101 will abolish the office of the Information Commissioner and amend the Data Protection Act 2018 accordingly. To ensure an orderly transfer of functions, the Information Commissioner's Office will not be abolished until the new body corporate, the Information Commission, is established.

Clause 102 provides for all regulatory and other functions of the Information Commissioner to be transferred to the new body corporate, the Information Commission, once it is established. The clause also provides for references to the Information Commissioner in enactments or other documents to be treated as references to the Information Commission, where appropriate, as a result of the transfer of functions to the new Information Commission.

Clause 103 will allow the Secretary of State to make a scheme for the transfer of property, rights and liabilities, including rights and liabilities relating to employment contracts, from the commissioner to the new commission. The scheme may transfer property such as IT equipment or office furniture, or transfer staff currently employed by the commissioner to the commission. The transfer scheme will be designed to ensure continuity and facilitate a seamless transition to the new Information Commission.

Schedule 13 will insert a new schedule 12A to the Data Protection Act 2018, which describes the nature, form and governance structure of the new body corporate, the Information Commission. The commission will be governed by an independent statutory board, which will consist of a chair and other non-executive members, as well as executive members including a chief executive. The new structure formalises aspects of the existing governance arrangements of the Information Commissioner's Office and brings the ICO in line with how other UK regulators, such as Ofcom and the Financial Conduct Authority, are governed. The chair of the new commission will be appointed by His Majesty by letters patent on the recommendation of the Secretary of State, as is currently the case for the commissioner.

Schedule 13 also provides for the current Information Commissioner to transfer to the role of chair of the Information Commission for the remainder of their term. I put on record the Government's intention to preserve the title of Information Commissioner in respect of the chair, in acknowledgment of the fact that the commissioner's brand is recognised and valued both domestically and internationally. Other non-executive members will be appointed by the Secretary of State, and the chief executive will be appointed by the non-executive members in consultation with the Secretary of State.

Government amendment 45 will allow the chair to appoint the first chief executive on an interim basis and for a term of up to a maximum of 24 months, which will minimise any delay in the transition from the commissioner to the new commission. As drafted, the Bill provides that the chief executive of the commission will be appointed by the non-executive members once they are in place, in consultation with the Secretary of State. The transition from the commissioner to the new Information Commission cannot take place until the board is properly constituted, with, as a minimum, a chair, another non-executive member and a chief executive in place. That requirement would be likely to cause delay to the transition, as the appointment of the non-executive members by the Secretary of State and the chief executive would need to take place consecutively.

Amendment 44 is a minor consequential amendment to paragraph 3(3)(a) of proposed new schedule 12A, making it clear that the interim chief executive is appointed as an executive member.

The amendments seek to minimise any delay in the transfer of functions to the new commission by enabling the appointment of the chief executive to take place in parallel with the appointments process for non-executive members. The appointment of the interim chief executive will be made on the basis of fair and open competition and in consultation with the Secretary of State. I commend clauses 100 to 103, schedule 13 and Government amendments 44 and 45 to the Committee.

Stephanie Peacock (Barnsley East) (Lab): It is a pleasure to serve under your chairship once again, Mr Hollobone. The clauses that restructure the Information Commissioner's Office are among those that the Opposition are pleased to welcome in the Bill.

The Information Commissioner is the UK's independent regulator for data protection and freedom of information under the Data Protection Act 2018 and the Freedom

of Information Act 2000. Under the current system, as the Minister outlined, the Information Commissioner's Office is a corporation sole, meaning that one person has overall responsibility for data protection and freedom of information, with a group of staff supporting them. However, as the use of data in our society has grown, so too has the ICO, from a team of 10 in 1984 to an organisation with more than 500 staff.

In that context, the corporation sole model is obviously not fit for purpose. Clauses 100 to 103 recognise that: they propose changes that will modernise the Information Commissioner's Office, turning it into the Information Commission by abolishing the corporation sole and replacing it with a body corporate. It is absolutely right that those changes be made, transforming the regulator into a commission with a broader set-up structure and a board of executives, among other key changes. That will bring the ICO in line with other established UK regulators such as Ofcom and the Financial Conduct Authority, reflect the fact that the ICO is not just a small commissioner's office, and ensure that it is equipped to deal with the volume of work for which it has responsibility.

It is essential that the ICO remains independent and fair. We agree that moving from an individual to a body will ensure greater integrity, although the concerns that I have raised about the impact of earlier clauses on the ICO's independence certainly remain. Overall, however, we are pleased that the Government recognise that the ICO must be brought in line with other established regulators and are making much-needed changes, which we support.

Question put and agreed to.

Clause 100 accordingly ordered to stand part of the Bill.

Schedule 13

THE INFORMATION COMMISSION

Amendments made: 44, in schedule 13, page 195, line 21, after "members" insert

"or in accordance with paragraph 23A".

This amendment is consequential on Amendment 45.

Amendment 45, in schedule 13, page 204, line 6, at end insert—

"*Transitional provision: interim chief executive*

23A (1) The first chief executive of the Commission is to be appointed by the chair of the Commission.

(2) Before making the appointment the chair must consult the Secretary of State.

(3) The appointment must be for a term of not more than 2 years.

(4) The chair may extend the term of the appointment but not so the term as extended is more than 2 years.

(5) For the term of appointment, the person appointed under sub-paragraph (1) is "the interim chief executive".

(6) Until the expiry of the term of appointment, the powers conferred on the non-executive members by paragraph 11(2) and (3) are exercisable in respect of the interim chief executive by the chair (instead of by the non-executive members).

(7) In sub-paragraphs (5) and (6), the references to the term of appointment are to the term of appointment described in sub-paragraph (3), including any extension of the term under sub-paragraph (4)."—*(Sir John Whittingdale.)*

The Bill establishes the Information Commission. This new paragraph enables the chair of the new body, in consultation with the Secretary of State, to appoint the first chief executive (as opposed to the appointment being made by non-executive members). It also enables the chair to determine the terms and conditions, pay, pensions etc relating to the appointment.

Schedule 13, as amended, agreed to.

Clauses 101 to 103 ordered to stand part of the Bill.

Clause 104

OVERSIGHT OF RETENTION AND USE OF BIOMETRIC MATERIAL

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

Sir John Whittingdale: Clause 104 will repeal the role of the Biometrics Commissioner and transfer the casework functions to the Investigatory Powers Commissioner. There is an extensive legal framework to ensure that the police can make effective use of biometrics, for example as part of an investigation to quickly and reliably identify suspects, while maintaining public trust. That includes the Police and Criminal Evidence Act 1984, which sets out detailed rules on DNA and fingerprints, and the Data Protection Act 2018, which provides an overarching framework for the processing of all personal data.

The oversight framework is complicated, however, and there are overlapping responsibilities. The Bio -metrics Commissioner currently has specific oversight responsibilities just for police use of DNA and fingerprints, while the Information Commissioner's Office regulates the use of all personal data, including biometrics, by any organisation, including the police. Clause 104 will simplify the framework by removing the overlap, leaving the ICO to provide independent oversight and transferring the casework functions to another existing body.

The casework involves extending retention periods in certain circumstances, particularly on national security grounds, and is quasi-judicial in nature. That is why clause 104 transfers those functions to the independent Investigatory Powers Commissioner, which has the necessary expertise, and avoids the conflict of interest that could occur if the functions were transferred to the ICO as regulator. Transparency in police use of biometrics is essential to retaining public trust and will continue through the annual reports of the Forensic Information Databases Service strategy board, the Investigatory Powers Commissioner and the ICO. I commend clause 104 to the Committee.

Stephanie Peacock: I will speak in more detail about my more general views on the oversight of biometrics, particularly their private use, when we come to new clauses 13, 14 and 15. However, as I look specifically at clauses 104 and 105, which seek to abolish the currently combined offices of Biometrics Commissioner and Surveillance Camera Commissioner, I would like to draw on the direct views of the Information Commissioner. In his initial response to "Data: a new direction", which proposed absorbing the functions of the Biometrics Commissioner and Surveillance Camera Commissioner into the ICO, the commissioner said that there were some functions that,

"if absorbed by the ICO, would almost certainly result in their receiving less attention".

Other functions, he said,

"simply do not fit with even a reformed data protection authority"

[Stephanie Peacock]

with there being

"far more intuitive places for them to go."

That was particularly so, he said, with biometric casework.

It is therefore pleasing that as a result of the consultation responses the Government have chosen to transfer the commissioner's biometric functions not to the ICO but to the Investigatory Powers Commissioner, acknowledging the relevant national security expertise that it can provide. However, in written evidence to this Committee, the commissioner reiterated his concern about the absorption of his office's functions, saying that work is currently being undertaken within its remit that, under the Bill's provisions, would be unaccounted for.

Given that the commissioner's concerns clearly remain, I would be pleased if the Minister provided in due course a written response to that evidence and those concerns. If not, the Government should at the very least undertake their own gap analysis to identify areas that will not be absorbed under the current provisions. It is important that this Committee and the office of the Biometrics and Surveillance Camera Commissioner can be satisfied that all the functions will be properly delegated and given the same degree of attention wherever they are carried out. Equally, it is important that those who will be expected to take on these new responsibilities are appropriately prepared to do so.

Sir John Whittingdale: I am happy to provide the further detail that the hon. Lady has requested.

Question put and agreed to.

Clause 104 accordingly ordered to stand part of the Bill.

Clause 105

OVERSIGHT OF BIOMETRICS DATABASES

Carol Monaghan (Glasgow North West) (SNP): I beg to move amendment 123, in clause 105, page 128, line 22, leave out subsections (2) and (3).

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

Clause stand part.

New clause 17—*Transfer of functions to the Investigatory Powers Commissioner's Office*—

"The functions of the Surveillance Camera Commissioner are transferred to the Investigatory Powers Commissioner."

Carol Monaghan: Society is witnessing an unprecedented acceleration in the capability and reach of surveillance technologies. Such an acceleration calls for protections and safeguards. Clause 105, however, does the opposite and seeks to abolish both the office of the Surveillance Camera Commissioner and its functions. The explanatory notes to the Bill state that the functions of the office of the Surveillance Camera Commissioner are duplicated and covered by the Information Commissioner's Office and its CCTV code of practice. That is not the case: the code is advisory only and is primarily concerned with data processes, not with actual surveillance.

Amendment 123 and new clause 17 would retain the functions of the Surveillance Camera Commissioner but transfer them to the Investigatory Powers Commissioner's Office, thus preserving those necessary safeguards. The IPCO already scrutinises Government activity and deals with the covert use of surveillance cameras, so dealing with overt cameras as well would be a natural extension of its function.

2.15 pm

Professor Pete Fussey of the University of Essex and Professor William Webster of the University of Stirling, who are directors of the Centre for Research into Information, Surveillance and Privacy, are considered the UK's leading experts on surveillance. They have conducted an independent review of the Bill as it relates to the functions of the Office of the Biometrics and Surveillance Camera Commissioner. Their view is that the Bill does not currently provide adequate mechanisms for the governance and oversight of surveillance cameras, including automatic number plate recognition, body-worn video, drones, facial recognition and so on, in comparison with the existing legislative arrangements under the Protection of Freedoms Act 2012.

It is important that any changes to current legislation preserve existing oversight and citizen safeguards, which are key to considering such intrusive types of technology. The Protection of Freedoms Act details provisions for the code of practice for surveillance camera systems and outlines the important functions for which the Surveillance Camera Commissioner is responsible:

"encouraging compliance with the surveillance camera code… reviewing the operation of the code, and…providing advice about the code (including changes to it or breaches of it)."

In addition to those statutory functions, Professor Fussey and Professor Webster highlight the importance of the Surveillance Camera Commissioner in relation to

"raising standards for surveillance camera developers, suppliers and users…and building legitimacy and consent for surveillance practices".

Furthermore, the commissioner reports annually to Parliament via the Home Secretary, which is an important mechanism for public trust in, and for the legitimacy of, the appropriate use of surveillance.

In his submission to the Committee, Professor Fraser Sampson, the Biometrics and Surveillance Camera Commissioner, highlights one particularly pressing role of his office at present, which relates to the procurement and use of Chinese surveillance technology. Although that role pertains to a significant national security priority, it is falling through the gaps of the Bill and has not been assigned to another office.

Clause 105 seeks to abolish the office of the Surveillance Camera Commissioner, while erasing its important functions. Considering the rapid advancement in surveillance technologies, including the concerning development and deployment of facial recognition technologies, it is more important than ever that we protect safeguards and build on them. My new clause 17 would preserve the important functions that I have outlined. The experts interviewed for Professor Fussey and Professor Webster's report supported such a change, highlighting how most of the gaps left in the Bill could be addressed if responsibility for the surveillance camera code were also moved under the IPCO.

Stephanie Peacock: Having outlined my broad concerns about clause 105 when I spoke to clause 104, I will focus briefly on the specific concern raised by the hon. Member

for Glasgow North West, which is that the Surveillance Camera Commissioner's functions will not be properly absorbed.

In evidence to the Committee, the commissioner outlined a number of non-data protection functions in relation to public space surveillance that their office currently carries out, but that, they believe, the Bill does not make provision to transfer. They cite the significant work that their office has undertaken to ensure that Government Departments are able

"to cease deploying visual surveillance systems onto sensitive sites where they are produced by companies subject to the National Intelligence Law of the People's Republic of China",

following a November 2022 instruction from the Chancellor of the Duchy of Lancaster. The commissioner says that such non-data protection work, which has received international acclaim, is not addressed in the Bill.

I am therefore hopeful that the explicit mention in amendment 123 that that the functions of the Surveillance Camera Commissioner will be transferred provides a backstop to ensure that all the commissioner's duties, including the non-data protection work, are accounted for. If the amendment is not accepted, a full-depth analysis should be conducted, as argued previously, with a full response issued to the commissioner's evidence to ensure that every one of the functions is properly and appropriately absorbed.

I understand the argument that the Surveillance Camera Commissioner's powers would be better placed with the Investigatory Powers Commissioner, rather than the ICO. Indeed, the commissioner's evidence to the Committee referenced the interim findings of an independent report it had commissioned, as the hon. Member for Glasgow North West just mentioned. The report found that most of the gaps left by the Bill could be addressed if responsibility for the surveillance camera code moved under the IPCO, harmonising the oversight of traditional and remote biometrics.

I end by pointing to a recent example that shows the value of proper oversight of the use of surveillance. Earlier this year, following a referral from my hon. Friend the Member for Bristol North West (Darren Jones), the ICO found a school in Bristol guilty of unlawfully installing covert CCTV cameras at the edge of their playing fields. Since then, the Surveillance Camera Commissioner has been responding to freedom of information requests on the matter, with more information about the incident thereby emerging as recently as yesterday. It is absolutely unacceptable that a school should be filming people without their knowledge. The Surveillance Camera Commissioner is a vital cog in the machinery of ensuring that incidents are dealt with appropriately. For such reasons, we must preserve its functions.

In short, I am in no way opposed to the simplification of oversight in surveillance or biometrics, but I hope to see it done in an entirely thorough way, so that none of the current commissioner's duties get left behind or go unseen.

Sir John Whittingdale: I am grateful to the hon. Members for Glasgow North West and for Barnsley East for the points they have made. The hon. Member for Glasgow North West, in moving the amendment, was right to say that the clause as drafted abolishes the role of the Surveillance Camera Commissioner and the surveillance camera code that the commissioner promotes compliance with. The commissioner and the code, however, are concerned only with police and local authority use in England and Wales. Effective, independent oversight of the use of surveillance camera systems is critical to public trust. There is a comprehensive legal framework for the use of such systems, but the oversight framework is complex and confusing.

The ICO regulates the processing of all personal data by all UK organisations under the Data Protection Act; that includes surveillance camera systems operated by the police and local authorities, and the ICO has issued its own video surveillance guidance. That duplication is confusing for both the operators and the public and it has resulted in multiple and sometimes inconsistent guidance documents covering similar areas. The growing reliance on surveillance from different sectors in criminal investigations, such as footage from Ring doorbells, means that it is increasingly important for all users of surveillance systems to have clear and consistent guidance. Consolidating guidance and oversight will make it easier for the police, local authorities and the public to understand. The ICO will continue to provide independent regulation of the use of surveillance camera systems by all organisations. Indeed, the chair of the National Police Data Board, who gave evidence to the Committee, said that that will significantly simplify matters and will not reduce the level of oversight and scrutiny placed upon the police.

Amendment 123, proposed by the hon. Member for Glasgow North West, would retain the role of the Surveillance Camera Commissioner and the surveillance camera code. In our view, that would simply continue the complexity and duplication with the ICO's responsibilities. Feedback that we received from our consultation showed broad support for simplifying the oversight framework, with consultees agreeing that the roles and responsibilities, in particular in relation to new technologies, were unclear.

The hon. Lady went on to talk about the oversight going beyond that of the Information Commissioner, but I point out that there is a comprehensive legal framework outside the surveillance camera code. That includes not only data protection, but equality and human rights law, to which the code cross-refers. The ICO and the Equality and Human Rights Commission will continue to regulate such activities. There are other oversight bodies for policing, including the Independent Office for Police Conduct and His Majesty's inspectorate of constabulary, as well as the College of Policing, which provide national guidance and training.

The hon. Lady also specifically mentioned the remarks of the Surveillance Camera Commissioner about Chinese surveillance cameras. I will simply point out that the responsibility for oversight, which the ICO will continue to have, is not changed in any way by the Bill. The Information Commissioner's Office continues to regulate all organisations' use of surveillance cameras, and it has issued its own video surveillance guidance.

New clause 17 would transfer the functions of the commissioner to the Investigatory Powers Commissioner. As I have already said, we believe that that would simply continue to result in oversight resting in two different places, and that is an unnecessary duplication. The Investigatory Powers Commissioner's Office oversees activities that are substantially more intrusive than those relating to overt surveillance cameras. IPCO's existing work requires it to oversee over 600 public authorities,

[Sir John Whittingdale]

as well as several powers from different pieces of legislation. That requires a high level of expertise and specialisation to ensure effective oversight.

For those reasons, we believe that the proposals in the clause to bring the oversight functions under the responsibility of the Information Commissioner's Office will not result in any reduction in oversight, but will result in the removal of duplication and greater clarity. On that basis, I am afraid that I am unable to accept the amendment, and I hope that the hon. Lady will consider withdrawing it.

Carol Monaghan: I thank the Minister for responding to my amendments. However, we have a situation where we are going from having a specialist oversight to a somewhat more generalist oversight. That cannot be good when we are talking about this fast-moving technology. I will withdraw my amendment for the moment, but I reserve the right to bring it back at a later stage. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 105 ordered to stand part of the Bill.

Clause 106

OVERSIGHT OF BIOMETRICS DATABASES

Stephanie Peacock: I beg to move amendment 119, in clause 106, page 130, line 7, leave out

"which allows or confirms the unique identification of that individual".

This amendment is intended to ensure that the definition of biometric data in the Bill includes cases where that data is used for the purposes of classification (and not just unique identification).

The Chair: With this it will be convenient to discuss new clause 8—*Processing of special categories of personal data: biometric data—*

"(1) Article 9 of UK GDPR is amended as follows.

(2) In paragraph (1), after "biometric data", omit "for the purpose of uniquely identifying a natural person."

This new clause would extend the same protections that are currently in place for the processing of biometric data for the purposes of identification to the processing of all biometric data, including if the processing is for the purpose of classification (i.e. identification as part of a group, rather than identification as an individual).

Stephanie Peacock: Biometric data is uniquely personal. It captures our faces, fingerprints, walking style, tone of voice, expressions and all other data derived from measures of the human body. Under current UK law, biometric data is defined as

"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person".

Furthermore, biometric data counts as special category personal data only when it is used or collected for

"the purpose of uniquely identifying a natural person".

However, as the use of biometrics grows, they are not only used for identification; indeed, there is a growing set of biometric technologies used to categorise or classify people on the basis of traits thought to be statistically related or correlated, however tenuously, with particular characteristics. For instance, biometric systems have been developed that attempt to infer people's sexuality from their facial geometry, or judge criminality from pictures of people's faces. Other biometric classification systems attempt to judge people's internal emotional state or intentions from their biometrics, such as tone, voice, gait or facial expressions, known as emotion recognition. For example, employers have used facial expression and tone analysis to decide who should be selected for a job, using biometric technologies to score candidates on characteristics such as enthusiasm, willingness to learn, conscientiousness and responsibility, and personal stability.

Members of the Citizens' Biometrics Council convened by the Ada Lovelace Institute in 2020 to build a deeper understanding of the British public's views on biometric technologies have expressed concerns about these use cases. Members suggest that these technologies classify people according to reductive, ableist and stereotypical characteristics, harming people's wellbeing and risking characterisation in a database or data-driven systems. Further, these cases often use pseudoscientific assumptions to draw links between external features and other traits, meaning that the underlying bases of these technologies are often not valid, reliable or accurate. For example, significant evidence suggests that it is not possible accurately to infer emotion from facial expressions. Despite that, existing data protection law would not consider biometric data collected for those purposes to be special category data, and would therefore not give data subjects the highest levels of safeguards in these contexts.

2.30 pm

The Ryder review, an independent legal review commissioned by the Ada Lovelace Institute and led by Matthew Ryder KC, identified that as a potential weakness in the existing regulatory regime. Ryder argued that the use of biometrics for classification or categorisation has the potential to be just as rights-intrusive as their use for unique identification, and that similarly high safeguards should therefore apply.

The Bill is an opportunity to remedy that oversight in existing data protection legislation. The amendment and new clause would ensure that it achieves that. It would extend the same protections currently in place for the processing of biometric data for the purposes of identification to the processing of all biometric data, including processing for the purpose of classification.

Sir John Whittingdale: Clause 106 makes changes to the national DNA database strategy board, which provides oversight of the operation of the national DNA database, including setting policies for access and use by the police. Amendment 119 would seem to extend the power to widen the board's potential scope beyond biometrics databases for the purpose of identification, to include the purpose of classification.

The police can process data only for policing purposes. It is not clear what policing purpose there would be in being able to classify, for example, emotions or gender, even assuming it was proven to be scientifically robust, or what sort of data would be on such a database. Even if one were developed in the future, it is likely to need knowledge, skills and resources very different from what is needed to oversee a database that identifies and eliminates suspects based on biometric identification, so it would probably make sense for a different body to carry out any oversight.

New clause 8 aims to make changes in a similar way to amendment 119 in relation to the definition of biometric data for the purposes of article 9 of the GDPR. As the GDPR is not concerned with the police's use of biometric data for law enforcement purposes, the new clause would apply to organisations that are processing biometric data for general purposes. The aim seems to be to ensure that enhanced protections afforded by GDPR to biometric data used for unique identification purposes also apply to biometric data that is used for classification or categorisation purposes.

The hon. Lady referred to the Ada Lovelace Institute's comments on these provisions, and its 2022 "Countermeasures" report issued on biometric technologies, but we are not convinced that such a change is necessary. One example in the report was using algorithms to make judgments that prospective employees are bored or not paying attention, based on their facial expressions or tone of voice. Using biometric data to draw inferences about people, using algorithms or otherwise, is not as invasive as using biometric data uniquely to identify someone. For example, biometric identification could include matching facial images caught on closed circuit television to a centrally held database of known offenders.

Furthermore, using biometric data for classification or categorisation purposes is still subject to the general data protection principles in the UK GDPR. That includes ensuring that there is a lawful ground for the processing, that the processing is necessary and proportionate, and is fair and transparent to the individuals concerned. If algorithms are used to categorise and make significant decisions about people based on their biometric characteristics, including in an employment context, they will have the right to be given information about the decision, and to obtain human intervention, as a result of the measures we previously debated in clause 11.

Therefore, we do see a distinction between the use of biometric information for identification purposes and the more general classification which the hon. Lady sought to draw. Though we believe that there is sufficient safeguard already in place regarding possible use of classification by biometric data, given what I have said, I hope that she will consider withdrawing the amendment.

Stephanie Peacock: I am grateful to the Minister for his comments. We will be speaking about the private uses of biometric data later, so I beg to ask leave to withdraw my amendment.

Amendment, by leave, withdrawn.

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

Sir John Whittingdale: DNA and fingerprints are key tools in helping the police to identify and eliminate suspects quickly and accurately by comparing evidence left at crime scenes with the appropriate files on the national databases. As I previously set out, clause 106 makes changes to the National DNA Database Strategy Board. The board provides oversight of the operation of the database, including setting policies for access and use by the police.

These reforms change the scope of the board to make it clear that they should provide similar oversight of the police fingerprint database, which operates under similar rules. The change brings the legislation up to date with the board's recently published governance rules. Clause 106 also updates the name of the board to the Forensic Information Databases Strategy Board, to better reflect the broadened scope of its work. We are also taking this opportunity to simplify and future-proof oversight of national police biometric databases. While DNA and fingerprints are well established, biometrics is an area of rapid technological development, including for example the growing use of iris, face and voice recognition. Given the pace of technological change in this area and the benefits of consistent oversight, Clause 106 also includes a power for the Secretary of State to make regulations which make changes to the board's scope, for example by adding new biometric databases into the board's remit or to remove them, where a database is no longer used. Such regulations would be subject to the affirmative procedure.

For these reasons, I commend the clause to the Committee.

Stephanie Peacock: Clause 106 will primarily increase the scope of the Forensic Information Databases Strategy Board to provide oversight of the national fingerprint database. However, there are also provisions enabling the Secretary of State to add or remove a biometric database that the board oversees, using the affirmative procedure. I would therefore like to ask the Minister whether they have any plans to use these powers regarding any particular databases—or whether this is intended as a measure for future-proofing the Bill in the case of changed circumstances?

I would also like to refer hon. Members to the remarks that I have made throughout the Bill that emphasise a need for caution when transferring the ability to change regulation further into the hands of the Secretary of State alone.

Sir John Whittingdale: I would add only that this is an area where technology is moving very fast, as I referred to earlier. We think it is right to put in place this provision, to allow an extension if it becomes necessary—though I do not think we have any current plans. It is future-proofing of the Bill.

Question put and agreed to.

Clause 106 accordingly ordered to stand part of the Bill.

Clause 107

REGULATIONS

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

The Chair: With this it will be convenient to discuss clauses 108 to 114 stand part.

Sir John Whittingdale: Clause 107 will give the Secretary of State a regulation-making power to make consequential amendments to other legislation. The power enables amendments to this Bill itself where such amendments are consequential to the abolition of the Information Commissioner and his replacement by the new Information Commission. Such provision is needed because there are a number of areas where data protection legislation will need to be updated as a consequence of the Bill. This is a standard power, commonly included in Bills to ensure that wider legislation is updated where necessary as a result of new legislation. For example, references to "the Commissioner" in the Data Protection Act 2018

[Sir John Whittingdale]

will no longer be accurate, given changes to the governance structure of the Information Commissioner's Office within the Bill, so consequential amendments will be required to that Act.

Clause 108 outlines the form and procedure for making regulations under the powers in the Bill: they are to be made by statutory instrument. Where regulations in the Bill are subject to the affirmative resolution procedure, they may not be made unless a draft of the statutory instrument has been laid before Parliament and approved by a resolution of each House. That provision is needed because the Bill introduces new regulation-making powers, which are necessary to support the Bill's policy objectives. For example, powers in part 3 of the Bill replace an existing statutory framework with a new, enhanced one.

Clause 109 explains the meaning of references to "the 2018 Act" and "the UK GDPR" in the Bill. Such provision is needed to explain the meaning of those two references. Clause 110 authorises expenditure arising from the Bill. That provision is needed to confirm that Parliament will fund any expenditure incurred under the Bill by the Secretary of State, the Treasury or a Government Department. It requires a money resolution and a Ways and Means resolution, both of which were passed in the House of Commons on 17 April.

Clause 111 outlines the territorial extent of the Bill. Specifically, the clause states that the Bill extends to England and Wales, Scotland and Northern Ireland, with some exceptions. Much of the Bill, including everything on data protection, is reserved policy. In areas where the Bill legislates on devolved matters, we are working with the devolved Administrations to secure legislative consent motions. Clause 112 gives the Secretary of State a regulation-making power to bring the Bill's provisions into force. Some provisions, listed in subsection (2), come into force on the date of Royal Assent. Other provisions, listed in subsection (3), come into force two months after Royal Assent. Such provision is needed to outline when the Bill's provisions will come into force.

Clause 113 gives the Secretary of State a regulation-making power to make transitional, transitory or saving provisions that may be needed in connection with any of the Bill's provisions coming into force. For example, provision might be required to clarify that the Information Commissioner's new power to refuse to act on complaints will not apply where such complaints have already been made prior to commencement of the relevant provision. Clause 114 outlines the short title of the Bill. That provision is needed to confirm the title once the Bill has been enacted. I commend clauses 107 to 114 to the Committee.

Stephanie Peacock: The clauses set out the final technical provisions necessary in order for the Bill to be passed and enacted effectively, and for the most part are standard. I will focus briefly on clause 107, however, as a number of stakeholders including the Public Law Project have expressed concern that, as a wide Henry VIII power, it may give the Secretary of State the power to make further sweeping changes to data protection law. Can the Minister provide some assurance that the clause will allow for the creation only of further provisions that are genuinely consequential to the Bill and necessary for its proper enactment?

It is my belief that this would not have been such a concern to civil society groups had there not been multiple occasions throughout the Bill when the Secretary of State made grabs for power, concentrating the ability to make further changes to data protection legislation in their own hands. I am disappointed, though of course not surprised, that the Government have not accepted any of my amendments to help to mitigate those powers with checks and balances involving the commissioner. However, keeping the clause alone in mind, I look forward to hearing from the Minister how the powers in clause 107 will be restricted and used.

Sir John Whittingdale: We have previously debated the efficacy of the affirmative resolution procedure. I recognise that the hon. Lady is not convinced about how effective it is in terms of parliamentary scrutiny; we will beg to differ on that point. Although the power in clause 107 allows the Secretary of State to amend Acts of Parliament, I can confirm that that is just to ensure the legal clarity of the text. Without that power, data protection legislation would be harder to interpret, thereby reducing people's understanding of the legislation and their ability to rely on the law.

Question put and agreed to.

Clause 107 accordingly ordered to stand part of the Bill.

Clause 108

Regulations

2.45 pm

Amendments made: 11, in clause 108, page 131, line 2, after "Act" insert

'made by the Secretary of State, the Treasury or the Welsh Ministers'.

This amendment is consequential on Amendments 8 and 10 and NC5.

Amendment 12, in clause 108, page 131, line 2, at end insert—

'(1A) For regulations under this Act made by the Scottish Ministers, see section 27 of the Interpretation and Legislative Reform (Scotland) Act 2010 (asp 10) (Scottish statutory instruments).'

This amendment is consequential on Amendments 8 and 10 and NC5.

Amendment 13, in clause 108, page 131, line 3, after "Act" insert

'made by the Secretary of State or the Treasury'.

This amendment is consequential on Amendments 8 and 10 and NC5.

Amendment 14, in clause 108, page 131, line 8, after "procedure" insert

'—

(a) if made by the Secretary of State or the Treasury,'.

This amendment is consequential on Amendments 8 and 10 and NC5.

Amendment 15, in clause 108, page 131, line 9, at end insert—

'(b) if made by the Scottish Ministers, the regulations are subject to the negative procedure (see section 28 of the Interpretation and Legislative Reform (Scotland) Act 2010 (asp 10));

(c) if made by the Welsh Ministers, the statutory instrument containing the regulations is subject to annulment in pursuance of a resolution of Senedd Cymru.'

This amendment is consequential on Amendments 8 and 10 and NC5. It makes provision about the meaning of the negative resolution procedure in connection with regulations made by Scottish Ministers or Welsh Ministers.

Amendment 16, in clause 108, page 131, line 10, after "Act" insert

'made by the Secretary of State or the Treasury'.—*(Sir John Whittingdale.)*

This amendment is consequential on Amendments 8 and 10 and NC5.

Clause 108, as amended, ordered to stand part of the Bill.

Clauses 109 to 114 ordered to stand part of the Bill.

New Clause 1

GENERAL PROCESSING AND CODES OF CONDUCT

'In Article 41 of the UK GDPR (monitoring of approved codes of conduct)—

(a) in paragraph 4, omit the words from ', including suspension' to the end, and

(b) after that paragraph insert—

"4A. If the action taken by a body under paragraph 4 consists of suspending or excluding a controller or processor from the code, the body must inform the Commissioner, giving reasons for taking that action."'.—*(Sir John Whittingdale.)*

This new clause clarifies that bodies accredited under Article 41 of the UK GDPR to monitor compliance with codes of conduct under Article 40 are only required to notify the Information Commissioner if they suspend or exclude a person from a code.

Brought up, read the First and Second time, and added to the Bill.

New Clause 2

CODES OF CONDUCT

'(1) The PEC Regulations are amended as follows.

(2) After regulation 32 insert—

"**Codes of conduct**

32A.—(1) The Commissioner must encourage representative bodies to produce codes of conduct intended to contribute to compliance with these Regulations.

(2) Under paragraph (1), the Commissioner must encourage representative bodies to produce codes which take account of, among other things, the specific features of different sectors.

(3) A code of conduct described in paragraph (1) may, for example, make provision with regard to—

(a) rights and obligations under these Regulations;

(b) out-of-court proceedings and other dispute resolution procedures for resolving disputes arising in connection with these Regulations.

(4) The Commissioner must encourage representative bodies to submit codes of conduct described in paragraph (1) to the Commissioner in draft.

(5) Where a representative body does so, the Commissioner must—

(a) provide the representative body with an opinion on whether the code correctly reflects the requirements of these Regulations,

(b) decide whether to approve the code, and

(c) if the code is approved, register and publish the code.

(6) The Commissioner may only approve a code if, among other things—

(a) the code contains a mechanism for monitoring whether persons who undertake to apply the code comply with its provisions, and

(b) in relation to persons other than public bodies, the mechanism involves monitoring by a body which is accredited for that purpose by the Commissioner under regulation 32B.

(7) In relation to amendments of a code of conduct that is for the time being approved under this regulation—

(a) paragraphs (4) and (5) apply as they apply in relation to a code, and

(b) the requirements in paragraph (6) must be satisfied by the code as amended.

(8) A code of conduct described in paragraph (1) may be contained in the same document as a code of conduct described in Article 40 of the UK GDPR (and a provision contained in such a document may be a provision of both codes).

(9) In this regulation—

'public body' has the meaning given in section 7 of the Data Protection Act 2018 (for the purposes of the UK GDPR);

'representative body' means an association or other body representing categories of—

(a) communications providers, or

(b) other persons engaged in activities regulated by these Regulations;

'the UK GDPR' has the meaning given in section 3(10) of the Data Protection Act 2018.

Accreditation of bodies monitoring compliance with codes of conduct

32B.—(1) The Commissioner may, in accordance with this regulation, accredit a body for the purpose of monitoring whether persons other than public bodies comply with a code of conduct described in regulation 32A(1).

(2) The Commissioner may accredit a body only where the Commissioner is satisfied that the body has—

(a) demonstrated its independence,

(b) demonstrated that it has an appropriate level of expertise in relation to the subject matter of the code,

(c) established procedures which allow it—

(i) to assess a person's eligibility to apply the code,

(ii) to monitor compliance with the code, and

(iii) to review the operation of the code periodically,

(d) established procedures and structures to handle complaints about infringements of the code or about the manner in which the code has been, or is being, implemented by a person,

(e) made arrangements to publish information about the procedures and structures described in sub-paragraph (d), and

(f) demonstrated that it does not have a conflict of interest.

(3) The Commissioner must prepare and publish guidance about how the Commissioner proposes to take decisions about accreditation under this regulation.

(4) A body accredited under this regulation in relation to a code must take appropriate action where a person infringes the code.

(5) If the action taken by a body under paragraph (4) consists of suspending or excluding a person from the code, the body must inform the Commissioner, giving reasons for taking that action.

(6) The Commissioner must revoke the accreditation of a body under this regulation if the Commissioner considers that the body—

(a) no longer meets the requirements for accreditation, or

(b) has failed, or is failing, to comply with paragraph (4) or (5).

(7) In this regulation, 'public body' has the same meaning as in regulation 32A.

Effect of codes of conduct

32C. Adherence to a code of conduct approved under regulation 32A may be used by a person as a means of demonstrating compliance with these Regulations.'

(3) In regulation 33 (technical advice to the Commissioner)—

(a) omit ', in connection with his enforcement functions,' and

(b) at the end insert 'where the request is made in connection with—

(a) the Commissioner's enforcement functions, or

(b) the Commissioner's functions under regulation 32A or 32B (codes of conduct).'

(4) In Schedule 1 (Information Commissioner's enforcement powers) (inserted by Schedule 10 to this Act), in paragraph 18(b)(ii) (maximum amount of penalty), for 'or 24' substitute ', 24 or 32B(4) or (5)".'.—*(Sir John Whittingdale.)*

This new clause inserts provision requiring the Information Commissioner to encourage representative bodies to prepare codes of conduct relating to compliance with the PEC Regulations and makes provision about the content of such codes.

Brought up, read the First and Second time, and added to the Bill.

New Clause 3

Information disclosed by the Welsh Revenue Authority

'(1) This section applies where the Welsh Revenue Authority discloses personal information to a person under section 54 for the purpose of enabling the person to provide digital verification services for an individual.

(2) The person must not further disclose the information otherwise than for the purpose of providing digital verification services for the individual, except with the consent of the Welsh Revenue Authority.

(3) Any other person who receives the information, whether directly or indirectly from the person to whom the Welsh Revenue Authority discloses the information, must not further disclose the information, except with the consent of the Welsh Revenue Authority.

(4) A person who discloses information in contravention of subsection (2) or (3) commits an offence.

(5) It is a defence for a person charged with an offence under subsection (4) to prove that the person reasonably believed—

(a) that the disclosure was lawful, or

(b) that the information had already lawfully been made available to the public.

(6) A person who commits an offence under subsection (4) is liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or a fine (or both);

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or a fine not exceeding the statutory maximum (or both);

(c) on summary conviction in Northern Ireland, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum (or both);

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or a fine (or both).

(7) In this section,

"personal information" means information relating to a person whose identity—

(a) is specified in the information, or

(b) can be deduced from it.'.—*(Sir John Whittingdale.)*

If the Welsh Revenue Authority discloses information under clause 54, this new clause prevents further disclosure of that information without the consent of the Welsh Revenue Authority.

Brought up, read the First and Second time, and added to the Bill.

New Clause 4

Information disclosed by Revenue Scotland

'(1) This section applies where Revenue Scotland discloses personal information to a person under section 54 for the purpose of enabling the person to provide digital verification services for an individual.

(2) The person must not further disclose the information otherwise than for the purpose of providing digital verification services for the individual, except with the consent of Revenue Scotland.

(3) Any other person who receives the information, whether directly or indirectly from the person to whom Revenue Scotland discloses the information, must not further disclose the information, except with the consent of Revenue Scotland.

(4) A person who discloses information in contravention of subsection (2) or (3) commits an offence.

(5) It is a defence for a person charged with an offence under subsection (4) to prove that the person reasonably believed—

(a) that the disclosure was lawful, or

(b) that the information had already lawfully been made available to the public.

(6) A person who commits an offence under subsection (4) is liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or a fine (or both);

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or a fine not exceeding the statutory maximum (or both);

(c) on summary conviction in Northern Ireland, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum (or both);

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or a fine (or both).

(7) In this section,

"personal information" means information relating to a person whose identity—

(a) is specified in the information, or

(b) can be deduced from it.'.—*(Sir John Whittingdale.)*

If Revenue Scotland discloses information under clause 54, this new clause prevents further disclosure of that information without the consent of Revenue Scotland.

Brought up, read the First and Second time, and added to the Bill.

New Clause 5

Meaning of "appropriate national authority"

'(1) In section 93, "appropriate national authority" means the Secretary of State, subject as follows.

(2) The Scottish Ministers are also an appropriate national authority in relation to regulations under section 93 which contain only provision which would be within the legislative competence of the Scottish Parliament if contained in an Act of that Parliament.

(3) The Welsh Ministers are also an appropriate national authority in relation to regulations under section 93 which contain only provision which would be within the legislative competence of Senedd Cymru if contained in an Act of the Senedd (ignoring any requirement for the consent of a Minister of the Crown).

(4) The consent of a Minister of the Crown is required before any provision is made by the Welsh Ministers in regulations under section 93 so far as that provision, if contained in an Act of Senedd Cymru, would require the consent of a Minister of the Crown.

(5) In Schedule 7B to the Government of Wales Act 2006 (general restrictions on legislative competence of Senedd Cymru), in paragraph 11(6)(b) (exceptions to restrictions relating to Ministers of the Crown)—

(a) omit the "or" at the end of sub-paragraph (viii), and

(b) after sub-paragraph (ix) insert "; or

(x) section 93 of the Data Protection and Digital Information Act 2023."

(6) In this section, "Minister of the Crown" has the same meaning as in the Ministers of the Crown Act 1975.'—*(Sir John Whittingdale.)*

This new clause makes provision about the exercise of the regulation-making power conferred by clause 93 on the Secretary of State, Scottish Ministers and Welsh Ministers. See also Amendments 8, 9 and 10.

Brought up, read the First and Second time, and added to the Bill.

New Clause 6

SPECIAL CATEGORIES OF PERSONAL DATA: ELECTED REPRESENTATIVES RESPONDING TO REQUESTS

'In paragraph 23 of Schedule 1 to the 2018 Act (special categories of personal data: elected representatives responding to requests), in sub-paragraph (4), for "fourth day after" substitute "period of 30 days beginning with the day after".'.—*(Sir John Whittingdale.)*

Schedule 1 to the Data Protection Act 2018 includes provision about certain processing of special categories of personal data by elected representatives. This new clause increases the period for which former members of the Westminster Parliament and the devolved legislatures continue to be treated as "elected representatives" following an election. See also Amendments 30 and 31.

Brought up, read the First and Second time, and added to the Bill.

New Clause 7

PRE-COMMENCEMENT CONSULTATION

'(1) A requirement to consult under section 83 may be satisfied by consultation before, as well as by consultation after, that section comes into force.

(2) A requirement to consult under a provision inserted into the PEC Regulations by any of sections 79 to 86 may be satisfied by consultation before, as well as by consultation after, the provision inserting that provision comes into force.'.—*(Sir John Whittingdale.)*

This new clause provides that requirements imposed by the Bill to consult under or in connection with the PEC Regulations can be satisfied by consultation which takes place before the relevant provision of the Bill comes into force.

Brought up, read the First and Second time, and added to the Bill.

New Clause 8

PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA: BIOMETRIC DATA

'(1) Article 9 of UK GDPR is amended as follows.

(2) In paragraph (1), after "biometric data", omit "for the purpose of uniquely identifying a natural person."'.—*(Stephanie Peacock.)*

This new clause would extend the same protections that are currently in place for the processing of biometric data for the purposes of identification to the processing of all biometric data, including if the processing is for the purpose of classification (i.e. identification as part of a group, rather than identification as an individual).

Brought up, and read the First time.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 4, Noes 9.

Division No. 28]

AYES

Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Whittingdale, rh Sir John
Eastwood, Mark	

Question accordingly negatived.

New Clause 9

TRANSPARENCY IN USE OF ALGORITHMIC TOOLS

'(1) The Secretary of State must by regulations make provision requiring Government departments, public authorities and Government contractors using algorithmic tools to process personal data to use the UK Algorithmic Transparency Standard.

(2) The UK Algorithmic Transparency Standard ("the Standard") is the standard published by the Central Digital and Data Office and Centre for Data Ethics and Innovation as part of the Government's National Data Strategy.

(3) Regulations under subsection (1) must require the publication of the information required by the Standard.

(4) Regulations under subsection (1) may provide for exemptions to the requirement for publication where necessary—

(a) to avoid obstructing an official or legal inquiry, investigation or procedure,

(b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties,

(c) to protect public security, or

(d) to safeguard national security.'—*(Stephanie Peacock.)*

This new clause puts legislative obligation on public bodies using personal data to use the UK Algorithmic Transparency Standard.

Brought up, and read the First time.

Stephanie Peacock: I beg to move, That the clause be read a Second time.

In order for the public to have trust in algorithmic decision making, particularly where used by the Government, they must be able to understand how and when it is being used as a basic minimum. That is something that the Government themselves previously recognised by including a proposal to make transparency reporting on the use of algorithms in decision making for public sector bodies compulsory in their "Data: a new direction" consultation. Indeed, the Government have already made good progress on bringing together a framework that will make that reporting possible. The algorithmic transparency recording standard they have built provides a decent, standardised way of recording and sharing information about how the public sector uses algorithmic tools. There is also full guidance to accompany the standard, giving public sector bodies a clear understanding of how to complete transparency reports, as well as a compilation of pilot reports that have already been published, providing a bank of examples.

However, despite that and the majority of consultation respondents agreeing with the proposed compulsory reporting for public sector bodies—citing benefits of increased trust, accountability and accessibility for the public—the Government chose not to go ahead with the legislative change. Relying on self-regulation in the early stages of the scheme is understandable, but having conducted successful pilots, from the Cabinet Office to West Midlands police, it is unclear why the Government now choose not to commit to the very standard they created. This is a clear missed opportunity, with the standard running the risk of failing altogether if there is no legislative requirement to use it.

As the use of such algorithms grows, particularly considering further changes contained in clause 11, transparency around Government use of big data and automated decision-making tools will only increase in importance and value—people have a right to know how they are being governed. As the Public Law Project argues, transparency also has a consequential value;

[Stephanie Peacock]

it facilitates democratic consensus building about the appropriate use of new technologies, and it allows for full accountability when things go wrong.

Currently, in place of that accountability, the Public Law Project has put together its own register called "Tracking Automated Government", or TAG. Using mostly freedom of information requests, the register tracks the use of 42 algorithmic tools and rates their transparency. Of the 42, just one ranked as having high transparency. Among those with low transparency are asylum estates analysis, used to help the Home Office decide where asylum interviews should take place, given the geographical distribution of asylum seekers across the asylum estate; the general matching service and fraud referral and intervention management system, used as part of the efforts of the Department for Work and Pensions to combat benefit fraud and error—for example, by identifying claimants who may potentially have undisclosed capital or other income; and housing management systems, such as that in Wigan Metropolitan Borough Council, which uses a points-based system to prioritise social housing waiting lists.

We all want to see Government modernising and using new technology to increase efficiency and outcomes, but if an algorithmic tool impacts our asylum applications, our benefits system and the ability of people to gain housing, the people affected by those decisions deserve at the very least to know how they are being made. If the public sector sets the right example, private companies may choose to follow in the future, helping to improve transparency even further. The framework is ready to go and the benefits are clear; the amendment would simply make progress certain by bringing it forward as part of the legislative agenda. It is time that we gave people the confidence in public use of algorithms that they deserve.

Sir John Whittingdale: I thank the hon. Member for Barnsley East for moving new clause 9. We completely share her wish to ensure that Government and public authorities provide transparency in the way they use algorithmic tools that process personal data, especially when they are used to make decisions affecting members of the public.

The Government have made it our priority to ensure that transparency is being provided through the publication of the algorithmic transparency recording standard. That has been developed to assist public sector organisations in documenting and communicating their use of algorithms in decision making that impacts members of the public. The focus of the standard is to provide explanations of the decisions taken using automated processing of data by an algorithmic system, rather than all data processing.

The standard has been endorsed by the Government's Data Standards Authority, which recommends the standards, guidance and other resources that Government Departments should follow when working on data projects. Publishing the standard fulfils commitments made in both the national data strategy 2020 and the national artificial intelligence strategy. Since its publication, the standard has been piloted with a variety of public sector organisations across the UK, and the published records can be openly accessed via gov.uk. It is currently being rolled out more widely across the public sector.

Although the Government have made it a priority to advance work on algorithmic transparency, the algorithmic transparency recording standard is still a maturing standard that is being progressively promoted and adopted. It is evolving alongside policy thinking and Government understanding of the complexities, scope and risks around its use. We believe that enshrining the standard into law at this point of maturity could hinder the ability to ensure that it remains relevant in a rapidly developing technology field.

Therefore, although the Government sympathise with the intention behind the new clause, we believe it is best to continue with the current roll-out across the public sector. We remain committed to advancing algorithmic transparency, but we do not intend to take forward legislative change at this time. For that reason, I am unable to accept the new clause as proposed by the Opposition.

Stephanie Peacock: I am grateful to the Minister, but I am still confused about why, having developed the standard, the Government are not keen to put it into practice and into law. He just said that he wants to keep it relevant; he could use some of the secondary legislation that he is particularly keen on if he accepted the new clause. As I outlined, this issue has real-life consequences, whether for housing, asylum or benefits. In my constituency, many young people were affected by the exam algorithm scandal. For those reasons, I would like to push the new clause to a vote.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 4, Noes 9.

Division No. 29]

AYES

Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Whittingdale, rh Sir John
Eastwood, Mark	

Question accordingly negatived.

New Clause 10

PROVISION ABOUT REPRESENTATION OF DATA SUBJECTS

'(1) Section 190 of the Data Protection Act 2018 is amended as follows.

(2) In subsection (1), leave out "After the report under section 189(1) is laid before Parliament, the Secretary of State may" and insert "The Secretary of State must, within three months of the passage of the Data Protection and Digital Information Act 2023,".'—*(Stephanie Peacock.)*

This new clause would require the Secretary of State to exercise powers under s190 DPA2018 to allow organisations to raise data breach complaints on behalf of data subjects generally, in the absence of a particular subject who wishes to bring forward a claim about misuse of their own personal data.

Brought up, and read the First time.

Stephanie Peacock: I beg to move, That the clause be read a Second time.

Overall, the aim of the GDPR is to ensure the effective and complete protection of data subjects. That protection cannot be considered effective or complete if people cannot seek justice, remedy and repair if an organisation processes personal data unlawfully. Therefore, there must be suitable methods of redress for all data and decision subjects in any suitable data protection regime. Bringing any kind of legal case is not something people take lightly. Cases can be lengthy, costly and, in many lower-level cases, seem disproportionate to the loss suffered or remedy available. That is no different in cases surrounding the misuse of personal data.

As the law stands, article 80(1) of the EU GDPR has been implemented in the UK, meaning a data subject has the right to mandate a not-for-profit body or organisation to lodge a complaint on their behalf. That means, for example, a charity can help an individual to bring forward a case where they have been materially impacted by a data breach. Such provisions help to ensure that those who have suffered an infringement can be supported in lodging a claim, and are not disincentivised by a lack of understanding, resources or cost. However, the UK has not yet adopted article 80(2), which goes one step further, allowing those same organisations to lodge a complaint independently of a data subject's mandate.

3 pm

Currently, where there has been a macro-level infringement, non-profit organisations have no right to lodge a complaint on behalf of the wide group of people impacted, unless an individual evidences the specific impact of the breach or infringement on them. If one individual is prepared to launch a case, an organisation can help: where many individuals are affected, if no one in particular has the evidence or resources to bring an individual case, that same organisation would not be able to lodge a complaint, even though the negative impact of such an infringement could be much larger, could have arisen by design and could have far-reaching consequences.

Organisations that champion the rights of consumers, such as Which?, Reset and 5Rights, strongly argue that an effective data protection redress framework requires a collective redress mechanism. They say that that would aid in creating an environment where data subjects have confidence in the way that organisations use their data and can be assured that processes are in place to protect their data rights if something goes wrong domestically or internationally.

Indeed, individual rights are not enough. In modern data processing, our data is used to make decisions about us individually and it is pooled together to analyse trends and predict behaviours across a whole population. In those cases where data is processed as a collective, producing collective outcomes, the people and communities impacted in turn deserve to have collective representations made on their behalf. That is particularly so in the workplace, where unions and other representative organisations can recognise the collective dimensions of data but do not currently have the access to act formally on their members' behalf. As the TUC recognises, that only increases the asymmetry between the power of employers to collect and use data relating to their workers and the inability of employees to control that data in return. The great strength of feeling about the lack of protections for workers in this Bill was demonstrated by the App Drivers and Couriers Union's "Kill the Data Bill" protest that took place on 18 May outside the Department for Science, Innovation and Technology building.

Introducing article 80(2) would help to deliver something positive for workers and deliver better accountability for all. However, in their call for evidence on implementing the article, the Government said that they believe that

"there is insufficient evidence of systemic failings in the current regime"

to warrant its introduction. That is despite the ICO itself being cited in the response as being broadly supportive of the intention of article 80(2). The regulator, it said,

"recognised that opt-out proceedings have the potential both to contribute to the protection of the rights of data subjects who may not be aware of the potential breaches of their data protection rights, and to raise awareness and understanding of data rights and data misuse."

Of course, there must be space to debate valid concerns around the measures. For example, some business groups expressed worries in the call for evidence that the article could increase litigation costs and insurance premiums during a period of economic uncertainty. However, non-profits, such as those that would be operating under the article, are restricted by their own lack of resources in times of uncertainty, and by their mandates. As such, they are likely to consider claims or other action only in limited circumstances where there is high merit. Such a change is therefore not likely to open the floodgates for unnecessary legal cases, or to give rise to a compensation culture, but will simply allow for cases to take place when they are necessary.

There are also valid concerns that a so called opt-out model could actually cut individuals out of the process if a legal claim is pursued without their knowledge, which would run counter to the principles of transparency. However, that could easily be resolved by ensuring that appropriate safeguards were in place so that any proceedings under article 80(2) are well publicised and give individuals the opportunity to opt out at their choice.

Systemic failings should not be needed to realise that collective redress, at a time when the impacts of data are indeed collective, is a fundamental part of being able to properly exercise one's data rights. New clause 10 acknowledges that and simply seeks to ensure that, as the use of large-scale data grows, communities and groups of people will have collective rights that reflect those that an individual has. Only then can our protection laws be considered effective and complete.

Sir John Whittingdale: I am grateful to the hon. Lady for setting out the purposes of the new clause. As she has described, it aims to require the Secretary of State to use regulation-making powers under section 190 of the Data Protection Act to implement article 80(2) of the UK GDPR. It would enable non-profit organisations with an expertise in data protection law to make complaints to the Information Commissioner and/or take legal action against data controllers without the specific authorisation of the individuals who have been affected by data breaches. Relevant non-profit organisations can already take such actions on behalf of individuals who have specifically authorised them to do so under provisions in article 80(1) of the UK GDPR.

[Sir John Whittingdale]

In effect, the amendment would replace the current discretionary powers in section 190 of the Data Protection Act with a duty for the Secretary of State to legislate to bring those provisions into force soon after the Bill has received Royal Assent. Such an amendment would be undesirable for a number of reasons. First, as required under section 189 of the Data Protection Act, we have already consulted and reported to Parliament on proposals of that nature, and we concluded that there was not a strong enough case for introducing new legislation.

Although the Government's report acknowledged that some groups in society might find it difficult to complain to the ICO or bring legal proceedings of their own accord, it pointed out that the regulator can and does investigate complaints raised by civil society groups even when they are not made on behalf of named individuals. Big Brother Watch's recent complaints about the use of live facial recognition technology in certain shops in the south of England is an example of that.

Secondly, the response concluded that giving non-profit organisations the right to bring compensation claims against data controllers on behalf of individuals who had not authorised them to do so could prompt the growth of US-style lawsuits on behalf of thousands or even millions of customers at a time. In the event of a successful claim, each individual affected by the alleged breach could be eligible for a very small payout, but the consequences for the businesses could be hugely damaging, particularly in cases that involved little tangible harm to individuals.

Some organisations could be forced out of business or prompted to increase prices to recoup costs. The increase in litigation costs could also increase insurance premiums. A hardening in the insurance market could affect all data controllers, including those with a good record of compliance. For those reasons, we do not believe that it is right to extend the requirement on the Secretary of State to allow individuals to bring actions without the consent of those affected. On that basis, I ask the hon. Lady to withdraw the motion.

Stephanie Peacock: Data is increasingly used to make decisions about us as a collective, so it is important that GDPR gives us collective rights to reflect that, rather than the system being designed only for individuals to seek redress. For those reasons, I will press my new clause to a vote.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 4, Noes 9.

Division No. 30]

AYES

Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Henry, Darren
Clarke, Theo	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Whittingdale, rh Sir John
Eastwood, Mark	

Question accordingly negatived.

New Clause 11

PRIVACY ENHANCING TECHNOLOGIES

'(1) Within six months of the passage of this Act, the Secretary of State must publish and lay before Parliament a report on the potential impact of privacy enhancing technologies on the use and protection of personal data.

(2) "Privacy enhancing technologies" are software and hardware systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.'—*(Stephanie Peacock.)*

This new clause would require the Secretary of State to publish a report on the potential impact of Privacy Enhancing Technologies.

Brought up, and read the First time.

Stephanie Peacock: I beg to move, That the clause be read a Second time.

Privacy enhancing technologies are technologies and techniques that can help organisations to share and use people's data responsibly, lawfully and securely. They work most often by minimising the amount of data used, maximising data security—for example by encrypting or anonymising personal information—or empowering individuals. One of the best-known examples of a PET is synthetic data: data that is modelled to reproduce the statistical properties of a real dataset when taken as a whole. That type of data could allow third-party researchers or processors to analyse the statistical outcomes of the data without having access to the original set of personal data, or any information about identifiable living individuals.

Another example of PETs are those that minimise the amount of personal data that is shared without affecting the data's utility. Federated learning, for example, allows for the training of an algorithm across multiple devices or datasets held on servers, so if an organisation wants to train a machine-learning model but has limited training data available, they can send the model to a remote dataset for training. The model will then return having benefited from those datasets, while the sensitive data itself is not exchanged or ever put in the hands of those in ownership of the algorithm. The use of PETs therefore does not necessarily exclude data from being defined as personal or falling within the remit of GDPR. They can, however, help to minimise the risk that arises from personal data breaches and provide an increased level of security.

The Government have positioned the Bill as one that seeks to strengthen the data rights of citizens while catalysing innovation. PETs could and should have been a natural area for the Bill to explore, because not only can such devices help controllers demonstrate an approach based on data protection by design and default, but they can open the door for new ways of collaborating, innovating and researching with data. The Royal Society has researched the role that PETs can play in data governance and collaboration in immense detail, with its findings contained in its 2023 report, which is more than 100 pages long. One of the report's key recommendations was that the Government should develop a national PET strategy to promote their responsible use as tools for advancing scientific research, increasing security and offering new partnership possibilities, both domestically and across borders.

It is vital to acknowledge that working with PETs involves risks that must be considered. Some may not be robust enough against attacks because they are in the

early stages of development, while others might require a significant amount of expertise to operate, without which their use may be counterproductive. It is therefore important to be clear that the amendment would not jump ahead and endorse any particular technology or device before it was ready. Instead, it would enshrine the European Union Agency for Cybersecurity definition of PETs in UK law and prompt the Government to issue a report on how that growing area of technology might play a role in data processing and data regulation in future.

That could include identifying the opportunities that PETs could provide while also looking at the threats and potential harms involved in using the technologies without significant expertise or technological readiness. Indeed, in their consultation response, the Government even mentioned they were keen to explore opportunities around smart data, while promoting understanding that they should not be seen as a substitute for reducing privacy risks on an organisational level. The report, and the advancing of the amendment, would allow the Government that exploration, indicating a positive acknowledgment of the potentially growing role that PETs might play in data processing and opening the door for further research in the area.

Even by their name, privacy enhancing technologies reflect exactly what the Bill should be doing: looking to the future to encourage innovation in tech and then using such innovation to protect citizens in return. I hope hon. Members will see those technologies' potential value and the importance of analysing any harms, and look to place the requirement to analyse PETs on the statute book.

Sir John Whittingdale: We absolutely agree with the Opposition about the importance of privacy enhancing technologies, which I will call PETs, since I spoke on them recently and was told that was the best abbreviation—it is certainly easier. We wish to see their use by organisations to help ensure compliance with data protection principles and we seek to encourage that. As part of our work under the national data strategy, we are already exploring the macro-impacts of PETs and how they can unlock data across the economy.

The ICO has recently published its draft guidance on anonymisation, pseudonymisation and PETs, which explains the benefits and different types of PETs currently available, as well as how they can help organisations comply with data protection law. In addition, the Centre for Data Ethics and Innovation has published an adoption guide to aid decision making around the use of PETs in data-driven projects. It has also successfully completed delivery of UK-US prize challenges to drive innovation in PETs that reinforce democratic values. Indeed, I was delighted to meet some of the participants in those prize challenges at the Royal Society yesterday and hear a little more about some of their remarkable innovations.

As the hon. Lady mentioned, the Royal Society has published reports on how PETs can maximise the benefit and reduce the harms associated with data use. Adding a definition of PETs to the legislation and requiring the Government to publish a report six months after Royal Assent is unlikely to have many advantages over the approach that the ICO, the CDEI and others are taking to develop a better understanding in the area. Furthermore, many PETs are still in the very early stages of their deployment and use, and have not been widely adopted across the UK or globally. A statutory definition could quickly become outdated. Publishing a comprehensive report on the potential impacts of PETs, which advocated the use of one technology or another, could even distort a developing market, and lead to unintended negative impacts on the development of what are promising technologies. For that reason, I ask the hon. Lady to withdraw the new clause.

3.15 pm

Stephanie Peacock: I am grateful to the Minister for his clarification on the pronunciation of the acronym. I acknowledge the points he made. I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

New Clause 13

Oversight of biometric technology use by the Information Commission

'(1) The Information Commission must establish a Biometrics Office.

(2) The Biometrics Office is to consist of a committee of three commissioners with relevant expertise, appointed by the Commission.

(3) The functions of the Biometrics Office are—

(a) to establish and maintain a public register of relevant entities engaged in processing biometric data;

(b) to oversee and review the biometrics use of relevant entities;

(c) to produce a Code of Practice for the use of biometric technology by registered parties, which must include—

(i) compulsory standards of accuracy and reliability for biometric technologies,

(ii) a requirement for the proportionality of biometrics use to be assessed prior to use and annually thereafter, and a procedure for such assessment, and

(iii) a procedure for individual complaints about the use of biometrics by registered parties;

(d) to receive and publish annual reports from all relevant entities, which must include the relevant entity's proportionality assessment of their biometrics use;

(e) to enforce registration and reporting by the issuing of enforcement notices and, where necessary, the imposition of fines for non-compliance with the registration and reporting requirements;

(f) to ensure lawfulness of biometrics use by relevant entities, including issuing compliance and abatement notices where necessary.

(4) The Secretary of State may by regulations add to the responsibilities of the Biometrics Office.

(5) Regulations made under subsection (4) are subject to the affirmative resolution procedure.

(6) For the purposes of this Part—

"biometric data" has the meaning given by section 106 of this Act (see subsection 13);

"relevant entity" means any organisation or body corporate (whether public or private) which processes biometric data, other than where the biometric processing undertaken by the organisation or body corporate is otherwise overseen by the Investigatory Powers Commissioner, because it is—

(a) for the purposes of making or renewing a national security determination as defined by s.20(2) Protection of Freedoms Act 2012; or

(b) for the purposes set out in s.20(6) Protection of Freedoms Act 2012.'.—*(Stephanie Peacock.)*

This new clause, together with NC14 and NC15, are intended to form a new Part of the Bill which creates a mechanism for the Information Commission to oversee biometric technology use by private parties.

Brought up, and read the First time.

Stephanie Peacock: 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 14—*Requirement to register with the Information Commission—*

'(1) Any relevant entity intending to process biometric data for purposes other than those contained in section 20(2) and section 20(6) of the Protection of Freedoms Act 2012 must register with the Information Commission prior to the deployment of the biometric technology.

(2) An application for registration must include an explanation of the intended biometrics use, including an assessment of its proportionality and its extent.

(3) All relevant entities must provide an annual report to the Biometrics Office addressing their processing of biometric data in the preceding year and their intended processing of biometrics in the following year .

(4) Each annual report must contain a proportionality assessment of the relevant entity's processing of biometric data in the preceding year and intended processing of biometric data in the following year.

(5) Any relevant entity which processes biometric data without having registered with the Information Commission, or without providing annual reports to the Biometrics Office, is liable to an unlimited fine imposed by the Information Commission.'

See explanatory statement to NC13.

New clause 15—*Private biometrics use prior to entry into force of the Act—*

'Any relevant entity engaged in processing biometric data other than for the purposes contained in section 20(2) and section 20(6) of the Protection of Freedoms Act 2012 prior to the entry into force of this Part must register with the Information Commission in accordance with section *[Requirement to register with the Information Commission*] within six months of the date of entry into force of this Part; and subsection (5) of that section does not apply to such an entity during that period.'

See explanatory statement to NC13. This new clause would provide a transitional period of six months for entities which were already engaged in the processing of biometric data to register with the Commission.

Stephanie Peacock: A wider range of biometric data is now being collected than ever before. From data on the way we walk and talk to the facial expressions we make, biometric data is now being collected and used in a wide range of situations for many distinct purposes. Great attention has rightly been paid to police use of facial recognition technology to identify individuals, for example at football matches or protests. Indeed, to date, much of the regulatory attention has focused on those use cases, which are overseen by the Investigatory Powers Commissioner. However, the use of biometric technologies extends far beyond those examples, and there has been a proliferation of biometrics designed by private organisations to be used across day-to-day life—not just in policing.

We unlock smartphones with our faces or fingerprints, and companies have proposed using facial expression analysis to detect whether students are paying attention in online classes. Employers have used facial expression and tone analysis to decide who should be selected for a job—as was already mentioned in reference to new clause 8. As the proliferation of biometric technologies occurs, a number of issues have been raised about their impact on people and society. Indeed, if people's identities can be detected by both public and private actors at any given point, there is potential for it to significantly infringe on someone's privacy to move through the world with freedom of expression, association and assembly. Similarly, if people's traits, characteristics or abilities can be automatically assessed on the basis of biometrics, often without a scientific basis, it may affect free expression and the development of personality.

Public attitudes research carried out by the Ada Lovelace Institute shows that the British public recognise the potential benefits of tools such as facial recognition in certain circumstances—for example, smartphone locking systems and in airports—but often reject their use in others. Large majorities are opposed to the use of facial recognition in shops, schools and on public transport, as well as by human resources departments in recruitment. In all cases, the public expect the use of biometrics to be accompanied by safeguards and limitations, such as appropriate transparency and accountability measures.

Members of the citizens' biometrics council, convened by the Ada Lovelace Institute in 2020 and made up of 50 members of the public, expressed the view that biometric technologies as currently used are lacking in transparency and accountability. In particular, safeguards are uneven across sectors. Private use of biometrics are not currently subject to the same level of regulatory oversight or due process as is afforded within the criminal justice system, despite also having the potential to create changes of life-affecting significance. As a result, one member of the council memorably asked:

"If the technology companies break their promises…what will the implications be? Who's going to hold them to account?"

It is with those issues in mind that experts and legal opinion seem all to come to the same consistent conclusion that, at the moment, there is not a sufficient legal framework in place to manage the unique issues that the private proliferation of biometrics use raises. An independent legal review, commissioned by the Ada Lovelace Institute and led by Matthew Ryder KC, found that current governance structures and accountability mechanisms for biometrics are fragmented, unclear and ineffective. Similar findings have been made by the Biometrics and Surveillance Camera Commissioner, and Select Committees in this House and in the other place.

The Government, however, have not yet acted on delivering a legal framework to govern the use of biometric technology by private corporations, meaning that the Bill is a missed opportunity. New clause 13 therefore seeks to move towards the creation of that framework, providing for the Information Commission to oversee the use of biometric technology by private parties, and ensure accountability around it. I hope that the Committee see the value of this oversight and what it could provide and will support the new clause.

Sir John Whittingdale: New clause 13 would require the Information Commission to establish a new separate statutory biometrics office with responsibility for the oversight and regulation of biometric data and technology. However, the Information Commissioner already has responsibility for monitoring and enforcing the processing of biometric data, as it falls within the definition of personal data. Under the Bill, the new body corporate—the

Information Commission—will continue to monitor and enforce the processing of all personal data under the data protection legislation, including biometric data. Indeed, with its new independent board and governance structure, the commission will enjoy greater diversity in skills and decision making, ensuring that the regulator has the right blend of skills and expertise at the very top of the organisation.

Furthermore, the Bill allows the new Information Commission to establish committees, which may include specialists from outside the organisation with key skills and expertise in specialist areas. As such, the Government are of the firm view that the Information Commission is best placed to provide regulatory oversight of biometric data, rather than delegating responsibility and functions to a separate office. The creation of a new body would likely cause confusion for those seeking redress, by creating novel complaints processes for biometric-related complaints, as set out in new clause 13(3)(c)(iii). It would also complicate regulatory oversight and decision making by providing the new office with powers to impose fines, as per subsection (2)(e). For those reasons, I encourage the hon. Lady to withdraw her new clause.

New clauses 14 and 15 would require non-law enforcement bodies that process biometric data about individuals to register with the Information Commissioner before the processing begins. Where the processing started prior to passage of the Bill, the organisation would need to register within six months of commencement. As part of the registration process, the organisation would have to explain the intended effect of the processing and provide annual updates to the Information Commissioner's Office on current and future processing activities. Organisations that fail to comply with these requirements would be subject to an unlimited fine.

I appreciate that the new clauses aim to make sure that organisations will give careful thought to the necessity and proportionality of their processing activities, and to improve regulatory oversight, but they could have significant unintended consequences. As the hon. Lady will be aware, there are many everyday uses of biometrics data, such as using a thumbprint to access a phone, laptop or other connected device. Such services would always ask for the user's explicit consent and make alternatives such as passwords available to customers who would prefer not to part with their biometric data.

If every organisation that launched a new product had to register with the Information Commissioner to explain its intentions and complete annual reports, that could place significant and unnecessary new burdens on businesses and undermine the aims of the Bill. Where the use of biometric data is more intrusive, perhaps involving surveillance technology to identify specific individuals, the processing will already be subject to the heightened safeguards in article 9 of the UK GDPR. The processing would need to be necessary and proportionate on the grounds of substantial public interest.

The Bill will also require organisations to designate a senior responsible individual to manage privacy risks, act as a contact point for the regulator, undertake risk assessments and keep records in relation to high-risk processing activities. It would be open to the regulator to request to see these documents if members of the public expressed concern about the use of the technology.

I hope my response has helped to address the issues the hon. Lady was concerned about, and I would respectfully ask her to not to press these new clauses.

Stephanie Peacock: It does indeed provide reassurance. On that basis, I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

The Chair: We now come to the big moment for the hon. Member for Loughborough. Weeks of anticipation are now at an end. I call her to move new clause 16.

New Clause 16

PROCESSING OF DATA IN RELATION TO A CASE-FILE PREPARED BY THE POLICE SERVICE FOR SUBMISSION TO THE CROWN PROSECUTION SERVICE FOR A CHARGING DECISION

'(1) The 2018 Act is amended in accordance with subsection (2).

(2) In the 2018 Act, after section 40 insert—

"**40A Processing of data in relation to a case-file prepared by the police service for submission to the Crown Prosecution Service for a charging decision**

(1) This section applies to a set of processing operations consisting of the preparation of a case-file by the police service for submission to the Crown Prosecution Service for a charging decision, the making of a charging decision by the Crown Prosecution Service, and the return of the case-file by the Crown Prosecution Service to the police service after a charging decision has been made.

(2) The police service is not obliged to comply with the first data protection principle except insofar as that principle requires processing to be fair, or the third data protection principle, in preparing a case-file for submission to the Crown Prosecution Service for a charging decision.

(3) The Crown Prosecution Service is not obliged to comply with the first data protection principle except insofar as that principle requires processing to be fair, or the third data protection principle, in making a charging decision on a case-file submitted for that purpose by the police service.

(4) If the Crown Prosecution Service decides that a charge will not be pursued when it makes a charging decision on a case-file submitted for that purpose by the police service it must take all steps reasonably required to destroy and delete all copies of the case-file in its possession.

(5) If the Crown Prosecution Service decides that a charge will be pursued when it makes a charging decision on a case-file submitted for that purpose by the police service it must return the case-file to the police service and take all steps reasonably required to destroy and delete all copies of the case-file in its possession.

(6) Where the Crown Prosecution Service decides that a charge will be pursued when it makes a charging decision on a case-file submitted for that purpose by the police service and returns the case-file to the police service under subsection (5), the police service must comply with the first data protection principle and the third data protection principle in relation to any subsequent processing of the data contained in the case-file.

(7) For the purposes of this section—

(a) The police service means—

(i) constabulary maintained by virtue of an enactment, or

(ii) subject to section 126 of the Criminal Justice and Public Order Act 1994 (prison staff not to be regarded as in police service), any other service whose members have the powers or privileges of a constable.

(b) The preparation of, or preparing, a case-file by the police service for submission to the Crown Prosecution Service for a charging decision includes the submission of the file.

(c) A case-file includes all information obtained by the police service for the purpose of preparing a case-file for submission to the Crown Prosecution Service for a charging decision."' —*(Jane Hunt.)*

This new clause adjusts Section 40 of the Data Protection Act 2018 to exempt the police service and the Crown Prosecution Service from the first and third data protection principles contained within the 2018 Act so that they can share unredacted data with one another when making a charging decision.

Brought up, and read the First time.

Jane Hunt (Loughborough) (Con): I beg to move, That the clause be read a Second time.

It is a pleasure to speak before you today, Mr Hollobone, and to move my new clause. I recently met members of the Leicestershire Police Federation, who informed me of its concerns regarding part 3 of the Data Protection Act 2018, which imposes unnecessary and burdensome redaction obligations on the police and taking them away from the frontline. I thank the Police Federation for providing me with the information I am going to discuss and for drafting the new clause I have tabled.

Part 3 of the 2018 Act implemented the law enforcement directive and made provision for data processing by competent authorities, including police forces and the Crown Prosecution Service, for "law enforcement purposes".

Although recital (4) to the law enforcement directive emphasised that the

"free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences…should be facilitated while ensuring a high level of protection of personal data,"

part 3 of the 2018 Act contains no provision at all to facilitate the free flow of personal data between the police and the CPS. Instead, it imposes burdensome obligations on the police, requiring them to redact personal data from information transferred to the CPS. Those obligations are only delaying and obstructing the expeditious progress of the criminal justice system and were not even mandated by the law enforcement directive.

The problem has arisen due to chapter 2 of part 3 of the 2018 Act, which sets out six data protection principles that, as I have mentioned, apply to data processing by competent authorities for law enforcement purposes. Section 35(1) states:

"The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair."

Section 35(2) states:

"The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a) the data subject has given consent to the processing for that purpose, or

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority."

The Police Federation has said that it is very unlikely that section 35(2)(a) will apply in this context. It has also said that, in the case of section 35(2)(b), the test of whether the processing is "necessary" is exacting, requiring a competent authority to apply its mind to the proportionality of processing specific items of personal data for the particular law enforcement purpose in question. Under sections 35(3) to (5), where the processing is "sensitive processing", an even more rigorous test applies, requiring among other things that the processing is "strictly necessary" for the law enforcement purpose in question. Section 37 goes on to state:

"The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed."

For the purposes of the 2018 Act, the CPS and each police force are separate competent authorities and separate data controllers. Therefore, as set out in section 34(3), the CPS and each police force must comply with the data protection principles. A transfer of information by a police force to the CPS amounts to the processing of personal data.

The tests of "necessary" and "strictly necessary" under the first data protection principle and the third data protection principle require a competent authority to identify and consider each and every item of personal data contained within information that it is intending to process, and to consider whether it is necessary for that item of personal data to be processed in the manner intended.

The Police Federation has explained that, when the police prepare a case file for submission to the CPS for a charging decision, the practical effect is that they have to spend huge amounts of time and resources on doing so. They go through the information that has been gathered by investigating officers in order to identify every single item of personal data contained in that information; decide whether it is necessary—or, in many cases, strictly necessary—for the CPS to consider each item of personal data when making its charging decision; and redact every item of personal data that does not meet that test.

3.30 pm

Furthermore, the National Police Chiefs' Council and the CPS have produced detailed guidance on the redaction process, which emphasises that the 2018 Act is a legal requirement and that the police and CPS do not have any special relationship that negates the need to redact and protect personal information. The combination of the requirements of the guidance and of the Act represents a huge amount of administrative work for police officers, resulting in hours of preparing appropriate redactions.

Picture the scene: an incident occurs, and 10 police officers go to it. As they arrive, they all turn on their body-worn cams. They speak to different people and view different backgrounds with the cameras. They gather all sorts of different data, CCTV footage, Ring footage—just name it—and have to redact each in real time afterwards. It can take weeks to deal with just one incident. That burden was highlighted in the 2022 annual review of disclosure by the Attorney General's Office, which recorded:

"We have heard evidence, from all members of the justice system but especially the police, that redaction of material for disclosure is placing a significant pressure on resources"

and that one police force had invested £1 million in a disclosure specialist team solely to deal with redaction.

Furthermore, inevitably, such work is carried out by relatively junior officers who have no particular expertise in data protection, and much of it may never even be

used by the CPS if the matter is not charged or the defendant pleads guilty before trial. Nationally, about 25% of cases that are submitted to the CPS are not charged. A significant proportion of that time and money could therefore be saved if the redaction of personal data by the police occurred after, rather than before, a charging decision had been made by the CPS.

That is exactly what my new clause would ensure happened. It inserts a proposed new section into the 2018 Act to exempt the police service and the CPS from complying with the first data protection principle—except in so far as that principle requires processing to be fair—or with the third data protection principle when preparing a case file for submission to the CPS for a charging decision, thereby facilitating the free flow of personal data between the police and the CPS. Where the CPS decides to charge, the case file would be returned to the police to carry out the redaction exercise before there is any risk of the file being disclosed to any person or body other than the CPS. In the 25% of cases where the CPS decides not to charge, the unredacted file would simply be deleted by the CPS.

My new clause would have no obvious disadvantages, as the security of the personal data would not be compromised and the necessary redactions would still be undertaken once a charging decision had been made. Furthermore, there are already provisions in the Bill designed to reduce the burden that part 3 of the 2018 Act imposes on law enforcement bodies. For example, as previously discussed, clause 16 will reduce the burden of the logging obligation in section 62 of the 2018 Act. The impact of those other provisions would be greatly enhanced if my new clause were also included in the Bill.

It is crucial that we do everything we can to ease the administrative burdens on police officers, so that we can free up thousands of policing hours and get police back on to the frontline, supporting communities and tackling crime. My new clause would go a long way to achieving that by facilitating the free flow of personal data between the police and the CPS, which would speed up the criminal justice process and reduce the burden on the taxpayer.

I hope not to have to press the new clause to a vote, and that the Minister will provide some encouragement that the issue will be resolved during progress of the Bill.

Stephanie Peacock: New clause 16 would amend section 40 of the Data Protection Act 2018, allowing police services to share unredacted data with the Crown Prosecution Service when it is making a charging decision. I am incredibly sympathetic to the aim that the hon. Member for Loughborough has set out, which is to get the police fighting crime on the frontline as much as possible. In oral evidence, Aimee Reed, director of data at the Metropolitan police, said that if the police could share information redacted before charging decisions were made, it would be "of considerable benefit". She said that that would

"enable better and easier charging decisions"

and

"reduce the current burden on officers"—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 58, Q126.]

That would allow them to focus their time on other things. It is therefore good to see that concept being explored in a new clause.

To determine the value of the change, we would like to see a full impact assessment of the potential risks and harms associated with it. I hope that that could be conducted with the intention of weighing the change against the actual cost of the current burden that police face in redacting data. Without such an assessment, it is hard to determine whether the benefit to the police would be proportionate to the impact or harms that might occur as a result of the change, particularly for the subjects of data involved. That is not to say that any change would not be beneficial, but perhaps more detail could be explored with regard to the proposal.

As I believe that this is the final time that I will speak in this Committee, may I say a few words of thanks?

The Chair: I think that you should wait for the next Question.

Stephanie Peacock: Okay, I will wait for the next Question. Thank you for your guidance, Mr Hollobone.

Sir John Whittingdale: I thank my hon. Friend the Member for Loughborough, who has been assiduous in pursuing her point and has set out very clearly the purpose of her new clause. We share her wish to reduce unnecessary burdens on the police as much as possible. The new clause seeks to achieve that in relation to the preparation by police officers of pre-charge files, which is an issue that the National Police Chiefs' Council has raised with the Home Office, as I think she knows.

This is a serious matter for our police forces, which estimate that about four hours is spent redacting a typical case file. They argue that reducing that burden would enable officers to spend more time on frontline policing. We completely understand the frustration that many officers feel about having to spend a huge amount of time on what they see as unnecessary redaction. I can assure my hon. Friend that the Home Office is working with partners in the criminal justice system to find ways of safely reducing the redaction burden while maintaining public trust. It is important that we give them the time to do so.

We need to resolve the issue through an evidence-based solution that will ensure that the right amount of redaction is done at the right point in the process, so as to reduce any delays while maintaining victim and witness confidence in the process. I assure my hon. Friend that her point is very well taken on board and the Government are looking at how we can achieve her objective as quickly as possible, but I hope she will accept that, at this point, it would be sensible to withdraw her new clause.

Jane Hunt: I thank the Minister greatly for what he has said, and for the time and effort that is being put in by several Departments to draw attention to the issue and bring it to a conclusion. I am happy that some progress has been made and, although I reserve my right to bring back the new clause at a later date, I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

The Chair: Hon. Members will be disappointed to hear that we have reached the final Question that I must put to the Committee.

Question proposed, That the Chair do report the Bill, as amended, to the House.

Stephanie Peacock: It has been a real pleasure to represent His Majesty's loyal Opposition in the scrutiny of the Bill. I thank the Minister for his courteous manner, all members of the Committee for their time, the Clerks for their work and the many stakeholders who have contributed their time, input and views. I conclude by thanking Anna Clingan, my senior researcher, who has done a remarkable amount of work to prepare for our scrutiny of this incredibly complex Bill. Finally, I thank you, Mr Hollobone, for the way in which you have chaired the Committee.

Sir John Whittingdale: May I join the hon. Lady in expressing thanks to you, Mr Hollobone, and to Mr Paisley for chairing the Bill Committee so efficiently and getting us to this point ahead of schedule? I thank all members of the Committee for their participation: we have been involved in what will be seen to be a very important piece of legislation.

I am very grateful to the Opposition for their support in principle for many of the objectives of the Bill. It is absolutely right that the Opposition scrutinise the detail, and the hon. Member for Barnsley East and her colleagues have done so very effectively. I am pleased that we have reached this point with the Bill so far unamended, but obviously we will be considering it further on Report.

I thank all my hon. Friends for attending the Committee and for their contributions, particularly saying "Aye" at the appropriate moments, which has allowed us to get to this point. I also thank the officials in the Department for Science, Innovation and Technology. I picked up this baton on day two of my new role covering the maternity leave of my hon. Friend the Member for Hornchurch and Upminster (Julia Lopez); I did so with some trepidation, but the officials have made my task considerably easier and I am hugely indebted to them.

I thank everybody for allowing us to get this point. I look forward to further debate on Report, in due course.

The Chair: May I thank all hon. Members for their forbearance during the passage of the Bill and thank all the officers of the House for their diligence and attention to duty? My one remaining humble observation is that if the day ever comes when a facial recognition algorithm is attached to the cameras in the main Chamber to assess whether Members are bored or not paying attention, we will all be in very big trouble.

Question put and agreed to.

Bill, as amended, accordingly to be reported.

3.41 pm

Committee rose.

Written evidence reported to the House

DPDIB33 Jonathan Sellors MBE, Legal Counsel and Company Secretary, UK Biobank (supplementary submission)

DPDIB34 Marie Curie

DPDIB35 techUK (supplementary submission)

DPDIB36 Information and Records Management Society

DPDIB37 Aviva

DPDIB38 Equality and Human Rights Commission

DPDIB39 TransUnion International UK Limited

DPDIB40 British Medical Association