Public Bill Committee on Digital Economy Bill – Information Commissioner's submission

Introduction

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003, as amended (PECR). She also deals with complaints under the Re-use of Public Sector Information Regulations 2015 (RPSI) and the INSPIRE Regulations 2009.

2. The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

3. This evidence will focus on those aspects of the Bill that fall within the Information Commissioner's direct regulatory remit or have an impact on the privacy of individuals. These are: digital government (part 5); the statutory direct marketing code (Part 6); and age verification for access to online pornography (Part 3).

Part 5: Digital government

4. The Commissioner has made clear her aim to improve public trust in the use of personal data and to encourage the public, private and third sectors to make transparency for citizens a priority for all organisations that collect and use personal data. Transparency and a progressive information rights regime work together to build trust and the Commissioner welcomes the efforts to put defined areas of data sharing on a clear footing. The Commissioner further believes that risks posed by complexity in the Bill need to be addressed, further enhancing transparency for the citizen where they understand what benefit they gain from appropriate sharing and use of their personal data.

5. The Commissioner recognises the potential benefits of justified and proportionate data sharing and how it can help improve the delivery of public services for the public and improve policy decision making within government. Citizens want improved, seamless online services from the public sector and this may require more effective sharing of data

between public authorities. It is important that any provisions that may increase data sharing inspire confidence in those who will be affected. ICO research shows that the public are concerned about who their data is shared with and reflect concerns that they have lost control over how their information is used. Even apparently well-meaning sharing of data such as GP patient records for medical research purposes can arouse strong opinions.

6. The Commissioner has long made it clear that data protection should not be a barrier to necessary and proportionate data sharing, and this is emphasised in the Commissioner's statutory Data Sharing Code of Practice[1]. Large scale sharing of personal data across government and beyond inevitably engages privacy concerns and must be shown to be justified and proportionate. This is particularly the case for proposals involving bulk data sharing and the use of big data analytics. As more data is shared ever more widely and big data analytics are used in complex and unexpected ways, it will be particularly important to consider from the outset the privacy risk, the possible impact on individuals, and how to promote transparency so that people understand how their data is going to be used.

7. There is a clear need for extensive data sharing to be accompanied by robust safeguards. Most of these will be set out in the codes of practice; the Commissioner welcomes the requirements in the Bill to consult her on these codes. It is also positive to see that the fraud and debt data sharing pilots will be subject to review. The Commissioner will consider whether the proposed safeguards in the codes are sufficient and align with data protection obligations when she is formally consulted.

8. The Commissioner is concerned, having seen draft versions of the codes of practice, that they lack consistency and overarching coherence with one another. From the perspective of those individual citizens whose data may be shared under these proposed powers, the complexity of a multi-code framework may diminish their understanding and trust in the public sector's use of their data. From the perspective of data protection practitioners in public authorities charged with deciding whether to share personal data, consideration of multiple codes for various purposes as well as the DPA could be confusing and foster a risk-averse approach to otherwise beneficial data sharing for the public good.

---

[1] ICO data sharing code of practice https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

9. The Commissioner would encourage the government to consider further work to develop consistency between the codes and align them more closely with the ICO's Data Sharing Code of Practice. To achieve this the Commissioner suggests the addition of a clause in the Bill that makes clear that the codes of practice established under Part 5 of the Bill will be subordinate to the ICO's statutory Data Sharing Code of Practice.

10. The need for greater transparency of data sharing is not effectively addressed the face of the Bill. Transparency needs to be effective for average citizens who will want to understand in simple terms what will happen to their data. Transparency remains a key requirement of the data protection even when a legal basis for the sharing is found in other legislation. The Commissioner has recently issued a new code of practice of privacy notices, setting out how transparency needs to work in the digital age. Whilst issues of how transparency needs to work in practice can be addressed in the codes of practice it is also important that the commitment is on the face of the Bill. The Commissioner therefore recommends that a reference to the ICO code of practice on privacy notices and transparency for individuals is made on the face of bill.

11. The new EU General Data Protection Regulation (GDPR) and Law Enforcement Directive were adopted in May 2016. The new rules will take effect from May 2018 onwards. The GDPR includes stronger provisions on processing only the minimum data needed, requirements on clear privacy notices, explicit requirements for data protection by design and default, and for carrying out Data Protection Impact Assessments (DPIAs). Although the government's arrangements for exiting the European Union have yet to be decided it seems likely that the GDPR will take effect before the UK leaves. The government will have to introduce national level derogations as part of implementation. If this is the case then there will have to be a thorough consideration of the impact of the new legal framework on all aspects of the Bill affecting data sharing, including implementation arrangements.

12. In the interim two year period, the DPA remains applicable. The Commissioner welcomes the emphasis that data sharing should not contravene the DPA. It is also encouraging to see that the package of legislative proposals has been designed to sit alongside, rather than override, existing powers or legislation which enable public authorities to access or disclose information. She also welcomes the Bill's permissive approach to providing legal gateways to enable data sharing rather than mandatory powers obliging public authorities to share. This positive, enabling approach to legislating for data sharing has advantages over automatic or mandatory obligations to share

government data and will enable organisations to make balanced decisions in line with the DPA on whether the proposed data sharing is justified and proportionate.

13. The Commissioner also supports efforts to constrain the powers in the Bill by enabling specific data sharing rather than a wide, generic power to share all government data. Parliament made it clear during the passage of the Coroners and Justice Act 2009 that it did not support a very broad generic power for public authorities to share data. However the Commissioner recognises that improvements can be made to legislation to enable more flexible and faster decisions though better data sharing within government.

14. Proportionality and necessity are key to ensuring data sharing complies with data protection and human rights law. By referring to 'objectives' and 'purposes' e.g in clause 35 the Bill does not directly correlate with these concepts.

15. The clauses contain provisions for Ministers to specify in the statutory instruments the names of the public authorities to be involved in the sharing but there is not a requirement to specify the nature of the data to be shared or the purpose for doing so. The Commissioner understands that this will provide more flexibility. However because of the potential impact on individuals, she would wish to see a requirement in the codes of practice that all aspects of the proposed data sharing activity are properly considered and clearly set out in published Privacy Impact Assessments (PIAs) prior to data sharing.

16. There is a reliance on codes of practice to provide additional details and safeguards. It is important that the proposed content of these codes is available for scrutiny during the parliamentary consideration of the Bill, so that the whole regulatory framework including any limitations is clear.

Definitions of personal information and other terminology

17. The Bill includes a number of definitions of types of data and the organisations that will share it, which differ from the terminology used in data protection legislation. The Commissioner does not seek to have a monopoly on the approach taken to defining the various types of data that will be used in the data sharing process but deciding what is and what is not 'personal data' under the DPA is a fundamental requirement and a definition more readily understood by practitioners. In the Commissioner's response to the Better Use of

Data consultation[2] it was explained that there were advantages in aligning the terminology, as far as possible, with that used in the DPA; otherwise there is a risk that practitioners will be confused about whether 'identified data' or 'personal information' as used in the clauses may or may not be personal data.

Exemptions from the limitation on using shared data

18. A number clauses in the Bill specify that information can be shared for the purposes of—

    (i) preventing serious physical harm to a person,

    (ii) preventing loss of human life,

    (iii) safeguarding vulnerable adults or children,

    (iv) responding to an emergency, or

    (v) protecting national security.

19. The Explanatory Notes explain that this is to facilitate sharing in circumstances where it is envisaged that a public authority in receipt of information in accordance with clause 48 "might need to use information shared for a pressing matter in the public interest or in the interests of an individual's well-being, namely preventing serious physical harm to a person,… safeguarding vulnerable adults or children" etc.

20. The exceptions in sub-paragraphs (i), (ii) and (iii) of paragraph (e), all seek to reflect the condition for fair processing set out in paragraph 3 of Schedule 3 DPA. However, the provisions of the DEB are drafted in far more general terms than those in the DPA. The relevant DPA conditions are concerned with the vital interests of the individual in circumstances where consent cannot be obtained, it is unreasonable to require the data controller to seek to obtain it or, consent has been unreasonably withheld. Importantly, the data may not be processed unless the processing is necessary to protect vital interests.

21. The DEB imposes no requirement that the processing must be necessary in order for one of the exceptions set out in section 49(2)(e) to apply. Where such processing is merely helpful, but not necessary, compliance with the DEB exception will not satisfy the DPA condition for processing sensitive personal data.

[2] ICO response to Cabinet Office consultation on better use of data, April 2016 https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1624084/ico-response-to-cabinet-office-consultation-better-use-of-data-20160421.pdf

22. Where the DEB allows the sharing of information for the prevention of serious physical harm or loss of human life, the sharing may well be taking place in circumstances where it is necessary to protect the vital interests of an individual. Such sharing is likely to be DPA compliant. However, the situation is much less clear in relation to the sharing of sensitive personal data for the purposes of 'safeguarding vulnerable adults or children'. Whether the sharing of information for this purpose will satisfy the paragraph 3, Schedule 3 DPA condition will depend on the detailed circumstances of the case. The reference to mere "well-being" in the Explanatory Notes is likely to create confusion. 'Well-being' is an ill-defined term and is likely to fall well-below the protection of vital interests referenced in the DPA condition.

23. The term well-being only appears in the Explanatory Notes to the DEB and not in the statute itself. Where the term well-being has been referenced in legislation, as in the 'Named Person' scheme in Part 4 of the Children and Young People (Scotland) Act 2014, there has been a successful challenge to the compatibility of the legislation with an individual's fundamental rights. In the case of The Christian Institute and others (Appellants) v The Lord Advocate (Respondent) (Scotland) [2016] UKSC 51 the Supreme Court considered the data sharing arrangements put forward in connection with the 'Named Person' scheme in Part 4 of the Children and Young People (Scotland) Act 2014 and found that they were incompatible with the rights of children, young persons and parents under Article 8 of the European Convention on Human Rights (Right to respect for private and family life). Specifically they found that the sharing was "not in accordance with the law" as Article 8 requires because the effects of the provisions were not sufficiently clear that a person could regulate their conduct, nor were there sufficient safeguards so as to avoid arbitrary interference with fundamental rights.

24. The codes of practice may be able to provide further guidance on how Bill will interface with the DPA and address these issues but the Commissioner is concerned that these issues are not addressed on the face of Bill.

25. Consequently, a statute provision purporting to override the rights of an individual may be subject to challenge where the effect of the provision is to breach the individual's fundamental rights.

Definitions of de-identified, anonymised and pseudonymised data

26. Under current data protection legislation, anonymised data – data from which no individual can be identified or is reasonably likely to be

identified – is not personal data and is not subject to the DPA. The ICO's 'Anonymisation Code of Practice'[3] explains the process of converting personal data into a 'safe' anonymised form and stresses the importance of assessing re-identification risk in particular circumstances. Although government departments or public bodies may need a power in the legislation to share and link de-identified data, provided this data is anonymised using the processes suggested in the ICO's code, these activities are not subject to the DPA if the de-identification process has effectively anonymised the data.

Definition of personal information

27. In the clauses relating to some of the strands of data sharing, the definition of 'personal information' differs from the definition of personal data provided in the DPA. This highlights the specific concerns about confusing definitions mentioned above. The definition of personal information appears to have been taken from section 39 of the Statistics and Registration Service Act 2007 ("SRA"). This would be a wider definition than that of personal data under the DPA. Most notably, the draft clauses define 'personal information' to include information which relates to a body corporate. Personal data, as defined in the DPA, only includes information about a living person where this person can be identified from those data and other information in the possession or likely possession of the data controller. It is also not clear in the clauses if 'personal information' includes information about deceased persons, which again is not covered by the DPA. While the government may want to include a wider definition of the 'personal information' to be shared, there is potential for confusion between 'personal data' and 'personal information'. Any confusion that is likely to arise may be exacerbated by the provisions in the Bill which identify the types of personal information to be excluded from certain of the data sharing powers. This could also have an impact on compensatory safeguards because the Commissioner only regulates the use of personal data defined in data protection legislation.

Safeguards

28. Large-scale data sharing will require robust compensatory safeguards; these include organisations being clear about the law through ensuring there is practical guidance, including statutory codes. These help compliance with the law and the implementation of safeguards. The Commissioner supported the emphasis in the government's Better Use of Data consultation on the importance of safeguards, including an extension of sanctions, statutory codes of practice, the use of PIAs

[3] https://ico.org.uk/media/1061/anonymisation-code.pdf

and the use of pilots for the fraud and debt data sharing proposals. She also welcomes the proposed involvement of her office, for example, through requirements to be consulted on codes and through to undertaking audits. There will be resource considerations that must be addressed to ensure that the system of supervision is sufficiently robust to inspire public confidence.

29. Given the reliance on codes of practice to provide additional details and safeguards, it is important that the likely content of these codes is available for scrutiny during the passage of the Bill so that the whole regulatory framework, including any limitations, is clear. It is also critical that these codes be kept up-to-date, and the Commissioner suggests a requirement be included in the provisions of the legislation to regularly review all of the codes.

30. Much is made of the benefits of data sharing and the effectiveness of compensatory safeguards. It is important that there is effective post legislative scrutiny to ensure these are realised in practice. The Commissioner believes there should be provisions requiring a review of the data sharing based upon the powers emanating from the Bill. This review should consider the benefits and the effectiveness of safeguards and be carried out within a defined timescale. This review should be conducted by a trusted independent party charged with producing a report to parliament.

Sanctions for unlawful disclosure

31. The Bill includes a new criminal offence of unlawful disclosures which is consistent with existing sanctions for HM Revenue and Customs (HMRC), the Department for Work and Pensions (DWP) and information held by the UK Statistics Authority (UKSA) and Office of National Statistics (ONS). This begs a number of questions about this sanction including who will enforce this offence and whether it will just apply to organisations relying on the new powers. The role of the Commissioner and the interplay between the new powers and existing sanctions is also not clear. It will be important for the government to work with the Commissioner and others to ensure enforcement powers are effective and proportionate and do not create any room for confusion or conflict.

32. There are a number of enforcement tools available to the Commissioner for taking action against organisations who breach the DPA. They include criminal prosecution, non-criminal enforcement and consensual audits. The Commissioner also has the power to serve a monetary penalty notice imposing a penalty of up to £500,000 for serious breaches of the DPA. If an organisation or an individual successfully re-identify data, then in DPA terms they would become

the data controller for that data. If they processed personal data without making relevant parties aware and there is a risk of harm to the individuals, then the Commissioner may take regulatory action, including the imposition of a civil monetary penalty up to the maximum allowable amount. However, a potential enforcement notice or civil monetary penalty may not be an effective tool in these cases.

33. There is merit in considering whether there should be a specific criminal offence in cases of deliberate re-identification of anonymised data. By way of global context, the Australian government has recently announced an amendment to its Privacy Act that creates a criminal offence for re-identifying government data that has been de-identified[4].

34. On some occasions it is not the data controller that is responsible for data protection breaches; it is an individual acting in contravention of an organisation's policies and procedures, or an individual who obtains information from an organisation without their knowledge or consent. Section 55 of the DPA makes it a criminal offence to knowingly or recklessly – and without the consent of the data controller – obtain, disclose, or procure the disclosure of personal data. This offence is currently punishable by fine only. Section 77 of the Criminal Justice and Immigration Act 2008 includes a provision for introducing custodial sentences for the DPA section 55 offence; this has not yet been commenced. The Commissioner continues to call for more effective deterrent sentences, including the threat of prison in the most serious cases, to be available to the courts to stop the unlawful use of personal data. Strengthening this sanction would make it more consistent with the proposed new criminal offence of non-disclosure.

35. It is important that the governance, safeguards and sanctions are effective as the potential risk arising from the retention of personal information is not an academic one. The National Audit Office (NAO) has recently published a report on protecting information across government[5] highlighting concerns about the number of security incidents and diverse approaches to handling these across government. This underscores the need for effective governance.

Privacy Impact Assessments (PIAs)

36. The Commissioner notes that organisations engaging in data sharing under the powers in the Bill will be required under the Codes of

[4] https://www.attorneygeneral.gov.au/Mediareleases/Pages/2016/ThirdQuarter/Amendment-to-the-Privacy-Act-to-further-protect-de-identified-data.aspx

[5] NAO report Protecting information across government https://www.nao.org.uk/wp-content/uploads/2016/09/Protecting-information-across-government.pdf

Practice to prepare PIAs in line with the ICO's Privacy Impact Assessment Code of Practice[6] and publish them for public scrutiny. She welcomes this safeguard, and notes that it could help data controllers prepare for new requirements for Data Protection Impact Assessments if the GDPR is to be implemented as appears likely.

37. There is no statutory requirement to produce PIAs under the present UK data protection regime. Although including the requirement for a PIA within any new legislation that has a privacy impact on individuals is preferable, it may be possible to have a requirement in a statutory code of practice instead. To ensure this happens in relation to the powers in the Digital Economy Bill, it is important that any legal provisions to share data in Part 5 of the Bill that require an accompanying code of practice maintain in their codes a requirement on the undertaking and publication of PIAs. The ICO would also call for the requirement for PIAs to be included on the face of the Bill.

Part 6: Statutory direct marketing code

38. The Commissioner welcomes the provision for a direct marketing code of practice which, while not legally binding, would be admissible in evidence and would have to be taken into account by the Commissioner, tribunals and courts in relevant cases.

39. The Commissioner continues to receive a significant volume of reports from the public about nuisance marketing calls and texts. In each of the last four years more than 160,000 such concerns were reported to the ICO, and the projected figures for this year are similar.[7]

40. The public need to be able to trust organisations who handle their data and they need to retain control over their data – both of these things are essential to build confidence and encourage participation in the digital economy. The continuing volume of reported concerns over nuisance calls and texts indicate that marketing preferences are one area where the public have lost such trust and control over the use of their details.

41. The Commissioner's current direct marketing guidance[8] was published in 2013 to clarify the law and promote good practice in this area, but it has no formal status. Replacing the guidance with a statutory code of practice would give the guidance greater weight, enable us to

---

[6] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[7] See https://ico.org.uk/action-weve-taken/nuisance-calls-and-messages/ for figures on latest trends in reported concerns
[8] https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

provide more certainty on key issues such as time limits and consent to marketing from specific third parties, and make it easier to take enforcement action against organisations who don't follow its provisions.

42. Placing the guidance on a statutory footing will also help to ensure that it sits at the top of a hierarchy of various industry codes (such as those produced by the Direct Marketing Association and the new Fundraising Regulator).

43. It is important to recognise that a direct marketing code will not solve the nuisance of unwanted marketing on its own. However, it would be a useful tool in the Commissioner's continued work to ensure that organisations understand and comply with the marketing rules.

Part 3: Age verification for access to online pornography

44. The Commissioner provided a more detailed response to the DCMS consultation[9]. As a starting point, the Commissioner's view is that it is not privacy intrusive for an individual to be able to prove who they are in a secure and reliable way – or to prove that they have a particular attribute (for example, that they are of a particular age). She sees the challenge as being how to restrict the access of children to material identified as harmful, without interfering unduly with – or having an unjustifiable adverse impact on - the lawful activities of others.

45. Any solution used needs to find a balance between verifying the age of individuals and minimising the collection and retention of personal data. It also needs to address in a proportionate way the issue of confirming that it is an adult using a device, or sitting at terminal equipment.

46. The Commissioner's concern is that any solution implemented must be compliant with the requirements of the DPA and PECR. The concept of 'privacy by design' would seem particularly relevant in the context of age verification – that is, designing a system that appropriately respects individuals' privacy whilst achieving the stated aim.

47. In practical terms, this would mean only collecting and recording the minimum data required in the circumstances, having assessed what that minimum was. It would also mean ensuring that the purposes for

[9] ICO response to DCMS consultation on child safety online: age verification for pornography April 2016 https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1623936/ico-response-to-dcms-consultation-on-child-safety-online-age-verification-for-pornography-20160412.pdf

which any data is used are carefully and restrictively defined, and that any activities keep to those restricted purposes.

48. In the context of preventing children from accessing online commercial pornography, there is a clear attribute which needs to be proven in each case – that is, whether an individual's age is above the required threshold. Any solution considered needs to be focussed on proving the existence or absence of that attribute, to the exclusion of other more detailed information (such as actual date of birth).

49. For example, the Commissioner would have significant concerns about any method of age verification that requires the collection and retention of documents such as a copy of passports, driving licences or other documents (of those above the age threshold) which are vulnerable to misuse and/or attractive to disreputable third parties. The collection and retention of such information multiplies the information risk for those individuals, whether the data is stored in one central database or in a number of smaller databases operated by different organisations in the sector.

50. Any solution must not result in the wholesale tracking or monitoring of individuals' lawful online activities, or the collection of data with a view to unlawful profiling of individuals.

Elizabeth Denham
Information Commissioner
12 October 2016