Data Reform Consultation Roundtable Focussing on the Privacy and Digital Rights of Individuals

Convened by the Privacy and Consumer Advisory Group (PCAG)[1] and the Open Rights Group[2]

Headline messages

- *Participants in this roundtable felt that the proposals typically saw data protection in terms of unnecessary burden on organisations (see 1.1, 2.1, 2.2 in this summary) rather than in terms of protecting individuals from harm arising from the use of personal data (1.3, 2.13, 5.9). Moreover, whilst the evidence of harm is increasingly apparent, the evidence of the regulatory burden is less clear cut (1.2, 2.1, 2.5) and often conflates issues arising from lack of clarity / understanding with existing regulations with limited organisational engagement in understanding the possible impacts of data flows (1.1) not only on individuals and their rights, but also on society.*
- *Given many data controllers will remain subject to GDPR requirements it is unclear how much divergence from existing (reasonably well) understood processes will result from the move to Privacy Management Programmes (2.3, 2.4, 2.5, 2.6, 2.7, 2.11). Additional insight into the consequences of heterogeneous privacy analyses for data subjects is probably warranted as is the cost of implementing another method for analysing privacy risks.*
- *Participants had particular concerns with proposals to remove data protection impact assessments and reforms of subject access requests (2.13).*
- *Participants highlighted a significant number of potential risks to the independence of the ICO (5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8).*
- *Care needs to be taken to align data protection proposals with other activities in the digital space including online safety / harms, digital identity and attributes trust framework and the digital markets unit (2.12).*

Process followed in Roundtable

This Roundtable took place on Zoom between 10.00 and 12.00 on 18 October 2021. It was held under the Chatham House rule and invitations were circulated via PCAG members, the ORG mailing list and social media. In addition to the roundtable organisers and HMG representatives, approximately 20 people participated in the roundtable including

1 https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group
2 https://www.openrightsgroup.org/

representatives from civil society, academia and industry. The Roundtable began with a quick poll that asked which chapters of the consultation had the most interest for participants. The poll indicated most interest in chapter 2, then chapter 1, then chapter 5, then chapter 4 and finally chapter 3. All chapters were discussed in the workshop.

This document presents a fuller response to the consultation than the summary prepared for the Minister in advance of the DCMS event on 3 November 2021.

For ease of analysis, this note presents the key points in numerical order of the chapters in the consultation. References to the consultation document are given in square brackets. Where participants made general comments rather than specific points these are presented inside quotation marks but may not be direct quotations from the roundtable, see Appendix.

Chapter 1 - Reducing barriers to responsible innovation

1.1. It was unclear how the proposals for research purposes [1.2] actually simplify the concerns of many research organisations, although the need for greater clarity was noted. As with other parts of the consultation, it is important to differentiate between the benefits of clarifying existing regulations and recommendations for new practices. This also needs to take into consideration the wealth of experience and expertise that has been developed around existing data use regulations and the additional complexity that might arise if new regulations are added to the mix.

1.2 The consultation on the ICO data sharing code of practice had a number of responses that asked for better guidance around data use in the research sector but there was no mention of respondents saying it was difficult for them to use data or a request for the legal basis to change.

1.3 There were concerns with the proposals around legitimate interests [1.4] noting that scrapping the balancing test shifts protections away from data subjects and towards controllers. More generally there was concern that the proposals subvert the purpose of data protection itself including purpose limitation.

1.4 There was a concern about potential ambiguities around the determination of legitimate interests being used as the basis for a data point in credit scoring, for example. This might require most contracts that touch digital systems across government services to be reviewed to ensure such unintended further uses are avoided.

1.5 More generally, the proposed revised list of legitimate interests [para 61] is very, very wide and very, very general. It also highlights the shift in perspective away from organisations demonstrating that their data use will not introduce harms but instead that they can find a predetermined legitimate interest that covers their activities.

1.6 There was a lack of clarity around the boundary between using data for training an AI program and using the data for business purposes [1.5] as well as concerns about how this

boundary would be enforced. There is a related concern about data used to monitor bias versus its use as training data.

1.7 The success of being able to use data for AI depends on increased public trust and willingness to share data. It is unclear whether the proposals will achieve this objective.

1.8 Indeed, if calling something AI means reduced oversight or regulatory burden there is a risk of polluting the good AI uses of data by using the term to cover a multitude of data uses.

Chapter 2 - Reducing burdens on businesses and delivering better outcomes for people

2.1 Participants shared the view that there was a lack of evidence of the burden on businesses (of all sizes) arising from GDPR and a real risk that claims about driving innovation end up subverting the meaning of data protection.

2.2 It was noted that data protection legislation has existed for over 30 years and therefore there is a wealth of expertise and support for working with the existing regulations, even if some aspects are ambiguous or poorly understood.

2.3 It was noted that many UK based companies, unless they are only dealing with UK customers and innovating for UK only solutions, will still need to comply with GDPR. For many companies, therefore, the proposals will mean that they will need to comply with GDPR and its associated processes AND the UK Privacy Management Programme [2.2] processes, thus increasing their regulatory burden rather than reducing it. The economic consequences of needing to comply with two regulatory regimes is likely to be felt disproportionately on smaller organisations rather than big technology companies and their existing consolidation of power.

2.4 Having two overlapping but essentially the same regimes also risks reducing legal certainty for all parties (although it increases the opportunities for legal services to resolve these issues in the UK).

2.5 Having to follow multiple rules risks giving extra lee-way that bad-faith actors will take advantage of and the good-faith actors won't need. More generally, any rules need to be simple because often the only people who can follow complex rules are criminals.

2.6 It is instructive to note that the proposal to replace Data Protection Impact Assessments with Privacy Management Programmes only appears in the consultation document under the generic heading of “Reform of the Accountability Framework” [2.2].

2.7 There were concerns that transparency and accountability (concepts with origins in Convention 108) would be much reduced under these proposals [2.2].

2.8 Whilst some stakeholders might see data protection impact assessments as bureaucratic box ticking exercises, when done well they encourage data controllers to think about what happens

to the data, where the data is going and the possible impacts of data flows on not only individuals and their rights, but also on society. As a consequence, the most effective assessments produce prose explanations of their systems, risks, harms and mitigations.

2.9 Arguably, the requirement to undertake Data Protection Impact Assessments for data sharing in response to COVID-19 meant that organisations thought carefully about what they were planning to do and why, as well as considering any potential risks from their proposals. As a consequence, few inappropriate or problematic data shares took place that might have undermined confidence in the use of health data.

2.10 If Privacy Management Programmes are to be effective, they should cover similar considerations to those covered by GDPR data protection impact assessments. If implemented poorly, they risk ending up simply replacing a GDPR box ticking exercise with a "British" box ticking exercise.

2.11 Allowing organisations complete flexibility in how they evaluate their own data risks via Privacy Management Plans may end up with two, equally undesirable, outcomes. The first will be a complete mish mash of methods, approaches, levels of integrity etc. which will increase the burden on data subjects choosing between different data controllers as well as making comparison across an industry sector difficult. Alternatively, an emerging market of Privacy Management Plan support might emerge which ends up offering commodified services with a tendency for a one-size-fits-all approach, or, at best, a set of industry specific services with little differentiation within a sector rather than the pragmatic, individualised approach implied by the proposals. Additionally, and certainly in the early stages, the approach to Privacy Management Plans is likely to mimic many of the steps involved in addressing GDPR.

2.12 Removing the requirement to designate a Data Protection Officer [para 163] needs to be considered in relation to other regulatory requirements for named roles, e.g. in relation to the Online Safety Bill as well as the Digital Identity and Attributes Trust Framework, Digital Markets Unit and the Plan for Digital Regulation.

2.13 Subject access requests [2.3] which are widely seen as a tool to promote transparency for organizations are now being seen as problematic in the consultation document, with data protection law now appearing to protect organisations from the concerns of data subjects rather than protecting data subjects from the harmful use of data.

2.14 It would be helpful to have more evidence of the scale of vexatious requests.

2.15 Given concerns about "surveillance capitalism" it is important to ensure that whilst removing cookie banners for necessary cookies is a sensible proposal, data subjects should continue to be informed about the use of intrusive tracking cookies [2.4].

Chapter 3 - Boosting trade and reducing barriers to data flows

3.1 There appears to be a lack of clarity in this section between exporting digital and data services and the transfer of data across borders [3.1]. Indeed, at times, some of the proposals seem to be of more benefit to third countries than to the UK[3] and further empirical analysis of the benefits to the UK economy would be beneficial.

3.2 Participants raised the concern that the discussion of adequacy was framed almost entirely in terms of supporting the free flow of data, whilst failing to acknowledge the important role of adequacy for recognising the steps taken by countries to provide adequate protections for personal data, particularly when they receive data from other countries.

3.3 Concerns were raised about the possibility of making adequacy decisions for groups of countries, regions or multilateral frameworks [3.2] as well as the potential for repetitive use of derogations [para 270] whereby the derogation becomes, effectively, business as usual. There were also concerns about the quality of the risk assessments that might be undertaken with concern that some companies may go over the edge with their own transfer mechanisms failing to meet the requirements for appropriate safeguards.

3.4 There is a risk that any proposed adequacy decision regarding data flows to the US might either end up unravelling in the face of emerging proposals for a federal privacy law or might cause problems for data sharing with the EU if there was a further Schrems ruling in that space.

3.5 The proposals seem to have given limited consideration to how alternative transfer mechanisms could be made simpler and cheaper to implement [3.3]. It would be helpful to have details of any early evaluations of the effectiveness of the New Zealand approach [described in para 264] which had been in operation for about nine months when the consultation was launched.

3.6 The consequences of these adequacy decisions for the UK-EU adequacy agreement may be significant and a more detailed impact assessment would be helpful.

Chapter 4 - Delivering better public services

4.1 Participants noted that there was relatively little detail in this part of the document but highlighted concerns that different government departments might seek to introduce special case exemptions for their own activities, thus undermining the intention behind these proposals. The fact that other government departments are planning to respond to the consultation suggests that it is less of a whole of government proposal than a DCMS led one.

3 In this context, see Durant, I. (2021). Developing countries and trade negotiations on e-commerce, *UNCTAD* (available at https://unctad.org/news/developing-countries-and-trade-negotiations-e-commerce).

4.2 It was unclear how these proposals relate to, for example, developments in the National Fraud Initiative including the recent consultation to expand the initiative by sharing more data[4].

4.3 There are various mentions of law enforcement and synergy with private sector organisations and co-operation [para 283] but limited discussion and participants felt that increased clarity on this point would be helpful.

Chapter 5 - Reform of the Information Commissioner's Office

5.1 There were no particular concerns with the reform of the broad organisational structure of the ICO (i.e. independent board and Chief Executive Officer) although it was felt to be important that the result of the reforms should be an independent, stronger ICO more willing to intervene rather than one who is less willing to intervene and has fewer effective powers. There is also a risk of the regulator becoming overburdened (especially with the existing Freedom of Information duties as well) and becoming less able to undertake any of its major duties.

5.2 The full implications of the proposed changes for the whole regulatory ecosystem need to be thought through. For example, prioritising amongst effectiveness, clarity, enforcement or increasing public trust in data use. Further complications arise because of the range of data related proposals being considered at the same time, including online safety / harms and digital markets unit as well as duties on the ICO for economic growth under the Deregulation Act 2015 that might be in conflict with their other duties, such as to support data rights or children's fundamental rights and freedoms[5].

5.3 The independence of the ICO is crucially important and the work of Graham Greenleaf[6] is particularly helpful in operationalising what independence should mean, to avoid some of the unfortunate examples within the EU where the independence of commissioners has been significantly undermined.

5.4 The risks to the independence of the ICO start with the appointment process and membership of the selection committee which should ideally reflect the range of policy objectives for the ICO (i.e. balancing the enforcement of privacy rights with the opportunities for new approaches to using data).

---

4 Cabinet Office (2021). Consultation on the expansion of the National Fraud Initiative (NFI) Data Matching Powers and the new Code of Data Matching Practice, *GOV.UK* (available at https://www.gov.uk/government/consultations/consultation-on-the-expansion-of-the-national-fraud-initiative-nfi-data-matching-powers-and-the-new-code-of-data-matching-practice).

5 E.g. O'Murchu, C. (2021). Facial recognition cameras arrive in UK school canteens, *FT* (available at https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9).

6 Greenleaf, G. (2012). Independence of data privacy authorities (Part I): International standards, *Computer Law & Security Review* 28(1), 3–13.

5.5 Concerns about the independence of the ICO also arise in relation to the move from parliamentary approval of the ICO's salary to allowing the Secretary of State to amend the salary [para 362].

5.6 Introducing a new power for the Secretary of State to prepare a statement of strategic priorities has been regarded by some as inappropriate even if an independent ICO were to use these to merely "inform" its own regulatory priorities. There was, instead, significant concern when these strategic priorities become associated with key performance indicators that are regularly reported on [5.4].

5.7 An independent ICO who, for example, chooses to focus its regulatory priorities on upholding data rights and encouraging trustworthy and responsible data use, but decides not to focus on the additional strategic priority around growth and innovation, might find its independence under significant pressure if its performance on the growth and innovation KPIs was poor.

5.8 Further threats to the independence of the ICO arise in relation to codes of practice and guidance [5.5] where, again, additional strategic priorities that the ICO might choose not to prioritise could still end up needing to be covered because they are specified in the list of required impact assessments.

5.9 Whilst there is a logic to requiring complainants to try to resolve their problems with the relevant data controller before reaching out to the ICO [5.6], participants were aware of the practical problems with this. For example, understanding who the relevant data controller was might be problematic and individuals may not feel confident in understanding the appropriate complaints process for each company (particularly if there is significant diversity of models arising from the PMPs).

5.10 Again, more detailed evidence of the level of "premature complaints" to the ICO would be helpful.

5.11 Participants noted that the biometrics commissioner was not consulted on the section of the consultation relating to their role [5.8]. The commissioner's own response highlights his surprise at the questions in this consultation that appeared a few days after he had responded to an earlier consultation[7].

Appendix: General comments about the consultation

"The chapter headings reflect the bias behind the proposals"

7 Biometrics and Surveillance Camera Commissioner (2021). DCMS consultation: "Data: a new direction": response by the Biometrics and Surveillance Camera Commissioner, *GOV.UK* (available at https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/dcms-consultation-data-a-new-direction-response-by-the-biometrics-and-surveillance-camera-commissioner-accessible-version).

"The whole thing assumes data protection is a 'burden' and that the benefits of collecting personal data outweighs the costs"

"Making the overall message 'data protection is a burden, we need to lighten that burden' is worrying"

"The high level messaging in this consultation is that there might be a problem for businesses in dealing with GDPR when in my experience this is not as much of a problem as is being presented, beyond cookie banners"

"Some regulatory 'barriers' aren't designed to block innovation, but to steer it away from inappropriate areas. There is a sense in the proposals that regulation is overwhelmingly seen as just a block on innovation"

"Does 'innovate' just mean 'collect data'[8]?"

"There is no substitute for not collecting the data in the first instance. Everything else is just privacy by promise, which is to say nothing at all"

"Are you saying that this proposal is really about encouraging the public to be comfortable with providing data, rather than to encourage businesses to collect less data in the first place?"

"If these proposals make it easier for data-harvesting companies to collect data, does that mean that government access to such data will also be easier?"

"The proposals should be moving towards higher levels of privacy protection, as our privacy is under increasing threat, rather than weakening it"

"There is a risk that that proposals will make data protection more like taxation - full of loopholes with a 'whack a mole', never ending, process to close them"

"Are we cynical enough to think that the primary purpose of this exercise is to relieve the government of the burden of data protection?"

"Maybe one of the solutions here is around proper enforcement of a regime rather than a new regime"

"I think it would be really bad to have two overlapping but essentially the same regimes for people to follow because it just gives more opportunity for legal wiggle room and and confusion all around and cost to business"

Georgia Meyer and Edgar Whitley
19 November 2021

8 Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology* 30(1), 75–89.