DATA PROTECTION AND DIGITAL INFORMATION BILL: BRIEFING NOTE

Missed opportunities

In the context of the first opportunity to reshape the UK's data protection regime since Brexit, there are a number of notable missed opportunities in the Data Protection and Digital Information Bill (the 'Bill') where data rights could have been enhanced, innovation facilitated, and the Government's stated objectives better met:

- The Bill fails to overcome one of the main barriers to data-driven research, the fact that those large controllers have no reason to share the data they hold with academic researchers.

- The Bill does not implement Article 80(2) in English law, which would have significantly improved standards of data protection by allowing representative bodies to bring complaints about breaches of the law;

- The Bill leaves the right to data portability unreformed and ineffective. This right not only has significant potential for business competition and innovation, but could help consumers realise the full benefits of decentralised digital technologies.

The Government should take this rare opportunity to make improvements to the UK's data protection regime that have long been advocated and would benefit researchers, individuals, and businesses.

Failure to incentivise *sharing* of data for research

1. The Bill's provisions on scientific research do not grapple with the principle current barrier to research processing in the GDPR: that it creates no incentive or obligation on the part of controllers to share data with third parties for scientific research. Given the risks (even if they are only notional) of sharing personal data with third party researchers, controllers with large amounts of data useful to researchers (such as social media platforms) have little reason to do so currently.

This dynamic has been articulated in a report by the European Digital Media Observatory, which both Meta/Facebook and Twitter themselves supported[1].

2. The Bill in practice gives greater freedom to *existing* controllers of large amounts of personal data to use their own data, without actively facilitating access to that data by independent researchers or other innovators. This puts a key objective of the Bill – to drive scientific research[2] - at serious risk.

3. The Bill could be improved by the inclusion of an incentive or obligation on certain specified types of data controller to make personal data available to independent researchers for public interest scientific research. Article 40 of the EU Digital Services Act (the 'DSA') provides an example of how this is being achieved elsewhere. The DSA obliges very large platforms to make data available to vetted researchers for academic research into systemic risks in the EU. The European Digital Media Observatory's draft code under Article 40 GDPR and accompanying report indicating how a system of researcher data access could be implemented in practice, including establishing an organisation dedicated to vetting researchers and reviewing and mediating their requests for access to specific datasets.

Improving privacy protection through representative actions

4. The aim of the GDPR is to ensure the "effective and complete" protection of data subjects[1]. Article 80 GDPR seeks to further that purpose by assisting data subjects to assert their rights.

5. Article 80(2) provides:

"Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in

[1] https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf
[2] https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation

Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing."

6. The intention behind Article 80(2) is to allow appropriately constituted organisations to bring proceedings concerning infringements of the data protection regulations in the absence of a data subject. That is, to ensure that proceedings may be brought in response to an infringement rather than on the specific facts of an individual's case. As a result, data subjects are – in theory – afforded greater and more effective protection of their rights.

7. Article 80(2) seeks to address infringements of the rights of data subjects at a macro level. Actions under it could address systemic infringements that arise by design, rather than requiring an individual to evidence the breaches and the specific effects to them.

Flaws in the existing Article 80(1) procedure

8. At present, an affected individual (a data subject) is always required in order to bring a claim or complaint to a supervisory authority. Indeed, the operation of data protection legislation is parasitic on a data subject. Whether through direct action or under s187 Data Protection Act 2018 ('DPA') (Representation of data subjects without their authority), a data subject will have to be named and engaged. In practice, a data subject is not always identifiable nor willing to bring action to address even the most egregious conduct.

9. Article 80(2) would fill a gap that Article 80(1) / s.187 DPA is not intended to fill. The Bill is the ideal opportunity for the Government to fully implement Article 80(2) GDPR in national law and plug a significant gap in the protection of UK citizens' privacy.

10. Article 80(2) recognises that there are instances where a data subject cannot be easily identified, or where a data subject might find it hard to evidence that they have been directly affected by the unlawful processing. Indeed, Article 80(1) / s.187 DPA is dependent on data subjects being sufficiently motivated by an identified (and identifiable) infringement of the data protection regulations. In practice, that process is not dissimilar to a data subject bringing such claims in

their own name. That data subject would also have to engage an appropriate non-profit organisation, who is ready, able and committed to bring such an action. This will require consideration of that non-profit's mandate, resources and capacity.

11. Furthermore, even a motivated data subject may be unwilling to take action due to the risks involved. For instance, it would be reasonable for that data subject to not want to become involved in a lengthy and costly legal process which may be disproportionate to the loss suffered or remedy available. This is particularly pressing where the infringement concerns systemic concerns rather than where an individual has suffered material or non-material damage as a result of the infringement.

What Article 80(2) could provide

12. Introducing Article 80(2) would help to obviate the difficulties and limitations associated with an Article 80(1) / s.187 DPA action, including the administrative and evidential difficulties that would currently be associated with signing individuals up to a representative action under Article 80(1).

13. Moreover, the relevant non-profit should not need to identify the data subjects affected under Article 80(2). Rather, Article 80(2) GDPR supports the "effective and complete" protection of the Regulation where the non-profit considers that the Regulation is being infringed.

14. The lack of redress for the illegality within the Advertising Technology (AdTech) industry is one good example of how non-profit action under Article 80(2) against actors in that industry could ensure "effective and complete" accountability for systemic infringements of the GDPR. Had Article 80(2) GDPR been introduced, then it is inevitable that an organisation could have brought proceedings against the issues inherent in AdTech, including cookie "pop-up" notices. Article 80(2) would allow the court's to engage with the systemic issues that AdTech presents.

Any increase in the level of complaints would likely be modest

15. Any fears of the implementation of Article 80(2) creating a "floodgates" scenario would be misplaced. Indeed, similar "floodgates" arguments were made in the Article 80(1) GDPR context[3] yet the predicted deluge of cases has not materialised. There are a number of practical barriers within s187 DPA to the introduction of such actions leading to a deluge of actions and claims:

i. An organisation has to meet two stringent qualifying criteria under §187 (3 – 4) DPA. Firstly, s.187(3) requires the organisation's constitution or enactment to have certain features including that it must be a non-profit and have objectives that are in the public interest. Secondly, s.187(4) DPA requires the organisation to be "active in the field of protecting data subjects' rights and freedoms with regard to the protection of their personal data". These criteria apply in an Article 80(1) context and should also apply to any action under Article 80(2).

ii. Non-profits are restricted by their own lack of resources, and their mandate. As such, they are only likely to consider claims or other action in limited circumstances. In particular, such organisations would only consider such claims where there is a particularly meritorious matter that would otherwise not be brought. This is a high internal barrier that will limit the use and abuse of the mechanism. As such, any prospect that non-profits would bring speculative or spurious claims is remote.

iii. Fears that a non-profit may "go rogue" and bring complaints or actions that a data subject would be dissatisfied with are similarly unfounded. Whichever mechanism is introduced would not enable the organisation to seek monetary redress for themselves or a data subject but rather to test the legality of practices.

iv. Properly constituted bodies will only bring such issues to the regulator or court where they have identified an infringement of the GDPR/DPA, which is within their mandate to consider, and where no other actor is bringing the action.

---

[3] See for instance Bird & Bird, 'The "Tidal wave" of data protection-related class actions: Why we're not drowning just yet…' (November 2018) < https://www.twobirds.com/en/news/articles/2018/global/tidal-wave-of-data-protection-related-cases> which observes that *"prior to the GDPR's entry into force in May this year, much was being said about the "inevitable" deluge of class actions likely to flood the UK court system as a result."*

v. While a non-profit may be able to bring a compensation action, depending on if and *how* Article 80(2) is introduced, it will not receive that compensation itself. This adds a further layer of protection should the ability to claim compensation for data subjects be granted to non-profits.

vi. For any damages claim, Article 82 GDPR requires a person to show material or non-material damage in order to be eligible for compensation. Non-profit organisations would not be able to show such damage, particularly where the damages regime is tied to individual data subjects. If the non-profit were able to show damages for individual data subjects, then they would be able to claim for damages in their own right under Article 82 which would obviate the need for an Article 80(2) process.

vii. Furthermore, the court system and regulatory oversight mechanisms are well versed in dealing with and filtering unmeritorious claims and actions. As such, this is a further barrier to such actions being misused.

viii. Finally, the costs risks of brining an action make cases and regulatory actions unlikely unless the organisation is willing to take those costs risks. Such risks will have to be weighed against the merit of the case and the lack of action by others to address the issue.

Making the right to data portability work

16. Article 20 GDPR gives data subjects the right to receive certain personal data which they have provided to a data controller, without hindrance and in an accessible format, and transmit that data to another controller. This is known as the right to "data portability".

17. The right to data portability is intended to provide a number of benefits to consumers, including the ability to have their data transferred from one data controller to another to another when switching, for example, between energy providers or banks. Consumers can also request their personal data from, for example, music and video streaming websites, including the data which users create when browsing or using such sites (for example, their search or viewing history). Finally, technology in theory permits users to aggregate and monetise

their own data through data unions and data trusts; a number of British companies are leading the development of such technology.

18. As currently formulated, however, the right to data portability is likely to be only of limited assistance to consumers. That limited right has not been enhanced in the Bill, contrasted to provision in the EU's Digital Markets Act which seek to augment and improve the right to portability.

The scope of Article 20

19. Article 20 GDPR provides (emphasis added):

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3.The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

20. A wide range of data held by controllers would constitute *"personal data concerning"* a data subject. As an example, personal data of a streaming site user (like their playlists and search history) is likely to be held in a way that relates

to the user in question, making it their personal data[4]. Such data is also likely to have been *"provided"* by the individual user to the streaming site platform. The scope of *"provided"* data is intended to include data which results from the observation of the user's activity.[5]

21. The relevant data will ordinarily be processed either on the basis of *"contract"* (i.e. the terms and conditions of use of the relevant streaming site) or *"consent"*, and for most sectors and services, will be carried out by *"automated means"*, thereby fulfilling the basic requirements of Article 20(1) GDPR.

Limitations on the right

22. First, the right does not allow for real-time and continued porting of data, limiting the ability of individuals to pool their data and maximise innovation using that data. While Article 20 does cover multiple data portability requests,[6] it is unlikely to *require* controllers to provide users with a continuous real-time flow of their personal data. Article 20 only entitles a streaming site user to receive their data in a *"structured, commonly used and machine-readable format"*. Beyond these minimum requirements, Article 20 does not impose specific conditions relating to how, or how often, the user's data should be provided (Guidelines, p.17).

23. Controllers can argue they are complying with Article 20 by providing users with an Excel spreadsheet of the data for example, which would hinder (or render impossible) the utilisation of such data in real-time. Whilst guidelines from data protection authorities suggest that the use of an externally accessible API may be *"a practical way"* of accommodating data portability, crucially they do not state that the use of such an API is, or can be, *required*. Many platforms now offer a "download your data" tool to data subjects, which may be used to achieve / show

[4] See e.g. *Nowak v Data Protection Commissioner* (Case C-434/16) [2018] 1 WLR 3505
[5] Article 29 Working Party Guidelines on the right to data portability ("**the Guidelines**"), pp.9-10
[6] Article 12(5) GDPR allows a data controller to charge a reasonable fee or to refuse to act on a request where this is "*manifestly unfounded or excessive*". However, the Guidelines state at p.12: "*There should be very few cases where the data controller would be able to justify a refusal to deliver the requested information, even regarding multiple data portability requests. For information society or similar online services that specialise in automated processing of personal data, it is very unlikely that the answering of multiple data portability requests should generally be considered to impose an excessive burden.*"

compliance with the right to portability, whilst limiting the practical utility of portability for data subjects.

24. Article 12(3) GDPR allows a data controller up to one month to respond to a data portability request and may allow up to three months in respect of complex and/or numerous requests. The specification of a defined (and relatively lengthy) response period further militates against interpreting Article 20 as conferring a right to real-time data portability.

25. It may further be disproportionate for a data subject to insist that their data be provided to them in a very specific format. While no express proportionality requirement is contained in Article 20, a court, tribunal or regulator may well use a proportionality analysis in practice[7]. Where users are seeking to monetise their data, that fact is likely to be relevant to any such proportionality assessment, given that a key (albeit not exclusive) focus of the right to data portability as it is currently formulated is to enable consumers to switch suppliers and/or service providers.

26. Thus, Article 20 is in practice a limited right that does not allow for innovative real-time porting and reuse of data.

27. Second, the right to data portability under Article 20 is conferred only on the individual users of streaming sites (i.e. the 'data subjects'), rather than on any third parties developing technology which enables real-time data porting.[8] Where a data subject mandates such third parties to act on their behalf, they will nevertheless be subject to the original controller's terms of service. If those terms preclude real-time data porting, third party developers would not be permitted to implement that technology on the relevant platform. This is likely to constitute a significant practical barrier to real-time porting by individual data subjects.

Recognition of limitations of the current regime

[7] See, by analogy, *Zaw Lin v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB). Although *Zaw Lin* concerned a request for information made under the (now repealed) Data Protection Act 1998, it illustrates that the court will be concerned to ensure that even data requests which engage fundamental rights are proportionate.

[8] Note that Article 20 is not covered within Article 80 GDPR, which allows for third party representation of data subjects in certain circumstances.

28. The current limitations on the right to data portability have recently been the subject of consideration by the European Commission[9]. The Commission recognised that *"as a result of its design to enable switching of service providers rather enabling data reuse in digital ecosystems the right has practical limitations"* (p.10). The strategy further notes that giving data subjects additional control over their personal data, including by facilitating real-time porting of such data, is likely to entail significant benefits for consumers, including by facilitating 'dynamic data portability' through decentralised digital technologies (pp.10-11 and p. 20). The Bill could and should seek to encourage such innovation, for the benefit of consumers and businesses.

Making the right to portability fit for purpose

29. The right to portability has serious limitations in that it does not allow consumers to port their data to third parties on a continuous, real-time basis. Addressing these shortcomings would make the right more useful and increase its use by consumers, promoting switching between services, competition, and innovation. It could also unlock models of consumer empowerment through decentralised technologies such as blockchain, and data trusts. The European Commission has indicated the right should be capable of expansion. The UK Government should take this opportunity to lead the way in updating the GDPR for the latest developments in digital technology.

[9] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *"A European Strategy for Data"* COM (2020) 66 https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf