Dr David Erdos—supplementary written evidence (FEO0097)

House of Lords Communications and Digital Committee inquiry into Freedom of Expression Online

During the hearing before the Committee on 19 January I was asked by a number of Members to follow-up my oral submission with further written evidence in relation to two matters

1. A Digital Authority?

The Chair, Lord Gilbert of Panteg, asked for further comments on the Committee's proposal for a Digital Authority which was a fundamental recommendation of its 2018-19 inquiry on *"The Internet: to regulate or not to regulate?"*.[1] The thrust of my evidence before the Committee was that even if the Government's December 2020 proposals for new Online Harms regulation through Ofcom[2] are implemented, the Information Commissioner's Office (ICO) will retain primary responsibility for defending privacy, reputation and other individual rights potentially negatively impacted by the processing of personal data online. That is clearly manifest as regards back-end processing but is also true in relation issues which may arise from the public dissemination of personal data. Thus, it is not only proposed that data protection *stricto senso* falls entirely outside of Ofcom's purview but that, outside of child protection and aside from category one services (the definition of which remains very unclear), Ofcom's remit will only extend to policing a duty of care as regards potential breaches of the criminal law. In contrast, most breaches of privacy, reputation and cognate rights are a matter of civil and/or regulatory law only. Alongside the ICO and Ofcom, the Competition and Markets Authority will also continue to exercise increasingly important duties to police anti-competitive practices and the ensure against the abuse of dominant positions.

It is vital that all three actors fulfil their regulatory tasks and are accountable for doing so. This includes being required to give an account to, and be scrutinized by, Parliament. However, that is intrinsically likely to be at most a broad-brush and indirect form of accountability. It is also crucial that the internal structuring of these regulators is fit for purpose in relation to the tasks which they must be perform and be held account for. Given the Information Commissioner's Office has so many myriad areas of work I think (as suggested by many others including Lord Justice Leveson) that that requires replacing the Commissioner-sole model with Commission model encompassing a group of Commissioners which could take a more thematic approach. Finally, at least in areas such as data protection regulation which strongly intersect with individual rights, it is

---

1 I did indeed submit written evidence to that inquiry. See http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-and-digital-committee/the-internet-to-regulate-or-not-to-regulate/written/82732.html. What I say here remains I hope broadly compatible with that as well as taking into account subsequent developments including the Committee's own inquiry Report.

2 See https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response.

crucial that this this is complemented by accountability vis-à-vis those who come forward with complaints. I say a bit more about this below when talking about enforcement.

Even if the above mechanisms were functioning well, there would undoubtedly be a number of tricky areas of overlap or other type of interaction. Overlap might be one of potential synergy or tension. For example, regulating to curtail the spread of revenge pornography online can be seen both as a matter of data protection and a matter of a future Ofcom-policed duty of care. In contrast, some of the tracking and artificial intelligence processes which could be mandated by Ofcom in relation potential terrorist or child abuse content may have a tense relationship with restrictions on such processing laid down in the UK General Data Protection Regulation. There is also the danger of an issue falling between regulatory gaps and, in this regard, there may also be the need for a certain amount of horizon scanning whereby regulators might see previously unforeseen concerns emerging and be able to flag these to policymakers. In all these areas, the concept of a digital authority or clearing house which brings regulators together in a joint board could have value. This board could also include representation from other bodies such as the Equality and Human Rights Commission and the Children's Commissioner which essentially only have an advisory function in relation to internet regulation. Along with the other three regulators I mentioned, it should also have a clear relationship with Parliament and there is merit in this regard to a new joint parliamentary committee as also put forward in the Committee's 2019 Report.

2. The Issue of Enforcement

Baroness Grender in particular asked for some further thoughts on enforcement. Similarly to the focus of my oral remarks, my comments here concern data protection enforcement by the Information Commissioner's Office (ICO). Given the sheer quantity of issues which fall within data protection and their great diversity in terms of seriousness and extent, a public regulator clearly cannot be expected to react formally to every complaint. Nevertheless, the GDPR (and now the UK GDPR) does establish an expectation of strong and systematic enforcement. Indeed, Recital 148 of the GDPR goes as far as to indicate that:

> *In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation.*

Moreover, in the binding C-311/18 *Schrems II* Grand Chamber judgment, the Court of Justice of the EU stated:

> *The supervisory authorities' primary responsibility is to monitor the application of the GDPR and to ensure its enforcement.* (at [108])

The realities are very different when it comes to UK regulation. Approximately three quarters of the ICO's resources are now dedicated to "proactive engagement activities",[3] leaving only around 25% for enforcement. This is

notwithstanding the acknowledged fact that it receives "high numbers of public complaints"[4] about data protection and related electronic privacy practices. Indeed, in 2019-20 it received approximately 40K data protection complaints,[5] as well as around 128K "concerns" under the Privacy and Electronic Communications Regulations.[6] Both of these figures were comparable to that of the previous year. In contrast, the Information Commissioner only invoked her formal enforcement powers a few handfuls of times. In sum, during 2019/20, the ICO issued "seven Enforcement notices, four cautions and eight prosecutions and fifteen fines".[7] Moreover, "the overwhelming majority of their [the ICO's] attention was directed against processing for direct marketing purpose" and also "data security shortcomings".[8] This leaves the great bulk of data protection complaints without any serious prospect of a formal regulatory response.

It is particularly concerning that a number of serious and systematic issues appear not to have been effectively addressed. One example is what often goes under the name of AdTech but might be better described as automated commercial services which systematically track, profile and seek to influence the behaviour of users online. As well as the general data protection regime, rules which specifically seek to ensure electronic privacy including as regards cookies have applied since 2003 and were toughened in 2009 to mandate that tracking for purely commercial reasons would require freely given opt-in consent. Since 25 May 2018, the GDPR has further strengthened the consent requirement. However, over this entire period a vast commercial ecosystem has developed which does not effectively meet relevant standards. Despite this, the ICO has made practically no use of its enforcement powers to address this. In September 2018 Jim Killock and Dr Michael Veale lodged a complaint ion relation to one important aspect of this issue, namely, real time bidding of user profiles. Refreshingly, the ICO not only investigated but in June 2019 confirmed the scale and import of the legal issues arising including that:

- *"Any processing of special category data [set out in Article 9 of the GDPR] is taking place unlawfully as explicit consent is not being collected (and no other condition applies)."*

- *"Processing of non-special category data is taking place unlawfully at the point of collection due to the perception that legitimate interests can be used for placing and/or reading a cookie or other technology."*

- *"The profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individuals' knowledge."*

---

3 See Information Commissioner's Annual Report and Financial Statements 2019-20, https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf, p. 35.

4 Ibid, p. 48.

5 Ibid, p. 50.

6 Ibid, p. 67,

7 Ibid, p. 35. Some of this action may have related to the Freedom of Information Act 2000 which clearly falls outside the scope of your inquiry.

8 Open Rights Group, *ICO Enforcement: Two Years After the GDPR* (25 January 2021), https://www.openrightsgroup.org/blog/ico-enforcement-two-years-after-the-gdpr/.

- *"Thousands of organisations are processing billions of bid requests in the UK each week with (at best) inconsistent application of adequate technical and organisational measures to secure the data in transit and at rest, and with little or no consideration as to the requirements of data protection law about international transfers of personal data."*

- *"Individuals have no guarantees about the security of their personal data within the ecosystem."*[9]

However, to date the ICO has still not enforced here and, even more concerningly, it reportedly closed the specific complaints in September 2020.[10] Whilst at least the former aspect may clearly be related to the Covid crisis and it is also the case that since I gave oral evidence the ICO's own work on AdTech has recommenced,[11] the general approach remains of concern. This is particularly the case as the ICO's work on this issue has been cited as something of a success story. For example, the Information Commissioner's evidence to the DCMS Sub-Committee on Online Harms and Disinformation stated on 26 January 2021 that:

> I think the UK is getting on top of this [internet advertising]. The Digital Markets Unit, the work that the Competition and Markets Authority is doing on investigating internet activities, *the work that we are doing to investigate real-time bidding that affects individuals*, I do think that regulators are getting on top of that.[12]

As I indicated in my oral evidence, there are many other significant areas where even less action has been in evidence. For example, in response to significant pressure including from The Law Society (see details in *The Law Society & Ors v Kordowski* [2011] EWHC 3185 (the *"Solicitors From Hell"* case) especially at [93]-[101]), the ICO issued guidance in 2013 which held that social networking sites and online forums did have controller responsibilities for the way they managed the public dissemination of third party personal data originating from other users. More specifically, this guidance stated that:

> *We would expect a person or organisation running a social networking site or online forum to have policies in place that are sufficient to deal with:*
>
> - *complaints from people who believe that their personal data may have been processed unfairly or unlawfully because they have been*

---

9 Information Commissioner's Office, *Update Report into Adtech and Real Time Bidding* (20 June 2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

10 Open Rights Group, *Privacy Organisation Open Rights taking the Privacy Regulator ICO to Court in a Landmark Case* (5 November 2020), https://www.openrightsgroup.org/press-releases/privacy-organisation-open-rights-group-taking-the-privacy-regulator-ico-to-court-in-a-landmark-case/.

11 Information Commissioner's Office, *Adtech Investigation Resumes* (21 January 2021), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/01/adtech-investigation-resumes/.

12 DCMS Committee Sub-Committee on Online Harms and Disinformation, *Oral Evidence: Online Harms and the Ethics of Data, HC 646*, https://committees.parliament.uk/oralevidence/1586/html/ at Q326 (emphasis added).

the subject of derogatory, threatening or abusive online postings by third parties; [and]

- *disputes between individuals about the factual accuracy of posts[.]*[13]

However, there has been no evidence of the use of the ICO's enforcement powers to police such standards since this time and no mention of any active enforcement strategy in subsequent ICO Annual Reports or other documentation.

Moving back to consider the broader picture, what is imperative is that a system is established for holding the ICO to account in a granular way for the exercise of its statutory duties and functions. A clear avenue for that to happen would be throughout the right of the individual under section 166 of the Data Protection Act 2018 to appeal to the First-Tier (or, in certain cases, Upper) Tribunal against an alleged failure of Information Commissioner "to take appropriate steps to respond to" a data protection complaint. That could only work, however, if the notion of appropriate steps was interpreted generously to include a substantive consideration of what investigation and also use of enforcement options would be appropriate in any given case for a public regulator with the tasks and broad set-up as the ICO. This would not confuse regulation with the civil courts but would be an important standard of accountability based on public law. Unfortunately, the Tribunal to date has interpreted section 166 in an extremely narrow and procedural fashion. I have tried to elucidate the problems with this in a recent piece in *European Data Protection Law Review*, the working paper version of which can be found online.[14] I am very pleased that the Open Rights Group is now challenging the Tribunal's approach in a new case[15] and is aware of my work in this regard. Should the Tribunal fail to revisit its approach then it would be important for Parliament to correct this through legislation. However, even if a broad approach was secured either through (in my opinion) a correction of case law or through legislative clarification, this would clearly only be a starting point to ensure that granular public law accountability become a systematic feature of the system.

16 February 2021

---

13 Information Commissioner's Office, *Social Networking and Online Forums – When Does the DPA* [Data Protection Act] *Apply?* (n.d./2013) https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf, p. 14.

14 See David Erdos, *Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?* (University of Cambridge Faculty of Law Research Paper No. 14/2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521372. The accepted version of the manuscript may also be requested via https://www.repository.cam.ac.uk/handle/1810/310820.

15 Open Rights Group, *Privacy Organisation Open Rights Group Taking the Privacy Regulator ICO to Court in a Landmark Case* (5 November 2020), https://www.openrightsgroup.org/press-releases/privacy-organisation-open-rights-group-taking-the-privacy-regulator-ico-to-court-in-a-landmark-case/.