Open Rights Group submission to the Department of Digital, Culture, Media and Sport

Plan for Digital Regulation

October 1, 2021

In this Submission

0. Executive Summary

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 20,000 active supporters, we are a grassroots organisation with local groups across the UK.

ORG welcome the opportunity to voice our concerns about Government Plans for Digital Regulation.

Firstly, we emphasise how framing outcomes in terms of “growth” and “innovation” fails to consider the partisan nature of technology, and how “new things” does not necessarily bring benefits for the individuals being affected by them.

Secondly, we compare how Government plans to gut data protection would effectively undermine other areas where the Government is trying to advance new regulations. “Data: a new direction” is the starkest product of Government ill-defined objectives, and a clear example of how this plan cannot achieve a coherent approach to digital regulation.

Thirdly, we emphasise the need of swift regulatory enforcement to drive market re-alignment. While we agree with Government plans to increase cooperation among Regulatory Authorities, we also emphasise the need to abandon the dysfunctional notion of “business-friendly” regulatory action and focus on effectiveness instead. Further, swift regulatory interventions and easy access to private enforcement and remedies are key for developing the principles enshrined in digital regulation, and create certainty over their application in practice.

Finally, we provide a short summary of our main takeaways and recommendations.

1. Innovation must be rooted in human rights

The UK Government "Plan for Digital Regulation" puts "Innovation at the heart of this Plan". This approach is reflected in the stated objectives of driving growth by promoting competition and innovation and the underpinning principle of actively promoting innovation.

However, innovation without any other connotation means merely new things, lacking any indication on whether these are desirable, able to solve existing problems, and benefit society as a whole. By failing to take this distinction into due account, this Plan fails to deliver a reasonable and coherent approach to Digital Regulation.

Firstly, this Plan focuses on promoting growth. However, evidence hardly indicates the need to stimulate investments or growth in the digital sector. For instance, a verbatim extract from the Plan reads as follow:

> *Digital technologies are the engine driving the UK's economic growth. The digital sector contributed £151bn in output and accounted for 1.6 million jobs in 2019. Over 34,000 new tech businesses were created in 2018 alone, and the UK attracted more international venture capital investment into technology businesses in 2020 than France and Germany combined.*

On the other hand, there is decisive and growing evidence that technology is either been weaponised against vulnerable individuals, or is otherwise resulting in negligent, unintended, adverse consequences for an increasing number of people. Without the pretence to draw an exhaustive picture, personal data is constantly being exploited to discriminate individuals' upon their weaknesses, anxieties,[1] opinions, or protected characteristics such as identity, race and gender.[2] Digital platforms overwhelmingly rely on business models whose financial sustainability depends on polarisation and misinformation,[3] thus harming social cohesion and the democratic discourse. Further, technology is leading to pervasive surveillance at

1 Panoptykon Foundation, *Algorithms of trauma: new case study shows that Facebook doesn't give users real control over disturbing surveillance ads*, at: https://en.panoptykon.org/algorithms-of-trauma

2 DataEthics, *The Inherent Discrimination of Microtargeting*, at: https://dataethics.eu/the-inherent-discrimination-of-microtargeting/

3 Privacy International, *The UN Report on Disinformation: a role for privacy*, at: https://www.privacyinternational.org/fr/node/4515

work,[4] in schools,[5] at home[6] and in public places,[7] as well as against journalists and activists.[8]

It follows that Government plans to focus on growth are ill-focused. Instead, the context we face requires boundaries and regulatory intervention to shift incentives, and ensure that growing investments in the digital sector result in the development and adoption of technologies that are ethical, transparent, and do bring benefits for society and the individuals concerned. For the same reasons, digital regulation need to strengthen safeguards and redress mechanisms for individuals who are victims of harm and other externalities. To achieve these objectives, regulation needs to be rooted in human rights and be designed to put human agency at the steering wheel.

The ill-conceived nature of the Government is embodied in their plans to water down the General Data Protection Regulation, as outlined in "Data: a new direction". Where the GDPR enshrined the objectives that "The processing of personal data should be designed to serve mankind" and "respect their fundamental rights and freedoms", the UK Government proposed framework is meant to "create an ambitious, pro-growth and innovation-friendly data protection regime" that unlocks the power of data across the economy. The prevalence of these aspects over rhetoric and unsubstantiated calls to secure a trusted data regime becomes obvious in the face of proposals that would provide unprecedented freedom to collect, use and share personal information, reduced transparency and increased bureaucracy for individuals seeking redress, as well as reduced accountability and oversight.

This approach is a recipe for disaster. The recent A-level failure should constitute a warning of what happens when safeguards, checks, and balances are considered optional or, perhaps, a form of bureaucratic excess standing in the path of innovation. When individuals feel unfairly treated, powerless to do anything about it, and without effective redress, public trust in government use of data is easily lost and not easily restored. The damage done in this instance, which rendered an entire generation with feelings of alienation from "the algorithm" and the government system around it, will adversely impact their trust in public use of their data for life.

4 Americal Civil Liberties Union, *Amazon Drivers Placed Under Robot Surveillance Microscope*, at: https://www.aclu.org/news/privacy-technology/amazon-drivers-placed-under-robot-surveillance-microscope/

5 Open Knowledge Foundation, *Open Knowledge Justice Programme challenges the use of algorithmic proctoring apps*, at: https://blog.okfn.org/2021/02/26/open-knowledge-justice-programme-challenges-the-use-of-algorithmic-proctoring-apps/

6 DataEthics, *Being Watched While Working From Home* at: https://dataethics.eu/being-watched-while-working-from-home/

7 Liberty, *Five Reasons Why Facial Recognition Must Be Banned*, at: https://www.libertyhumanrights.org.uk/issue/five-reasons-why-facial-recognition-must-be-banned/

8 The Guardian, *Huge data leak shatters the lie that the innocent need not fear surveillance*, at: https://www.theguardian.com/news/2021/jul/18/huge-data-leak-shatters-lie-innocent-need-not-fear-surveillance

Finally, we ought to emphasise that plans to undermine data protection in the UK would effectively frustrate Government plans to "promote competition across the digital sector", and "keep the UK safe and secure online".

1.1 The interplay between data protection and the new pro-competition regime

Plans to require dominant digital platforms to make their services interoperable with competitors would, in principle, entail clear benefits for individuals and society as a whole. Consumers would benefit from genuine choice, SMEs would benefit from reduced barriers to entry to digital markets, and increased putting competitive pressure on platforms would better support privacy and freedom of expression in their products.

These outcomes can be achieved only and insofar market players will use interoperability to offer better products, and compete on merit. In turn, this requires personal data being transferred from one service to another to be used only for the purposes of enabling interoperability and offering the service or product consumers meant to ask. However, Government plans to allow the re-use of personal data for other reasons than those they were originally collected for will introduce a different incentive, where companies are allowed to siphon and exploit personal data for commercial or other economic interests. In turn, this would harm consumers, saw distrust in the digital economy, and ultimately discourage multi-homing and reliance on interoperable products.

Evidence supports these conclusions. On the one hand, Open Banking found a success factor in their standardised APIs, that "had an impressive security record, with no mass data breaches occurring since its rollout".[9] In turn, data security undoubtedly contributed to consumer trust toward Open Banking, which is now regarded as a success model to be replicated and extended to digital markets.

On the other hand, structural insecurity in Real-Time-Bidding, the process that underpins digital advertising, resulted in a toxic and dysfunctional market rigged with fraud, harm and market abuses. In turn, data-driven advertising is widely regarded as a market failure: up to 97% of users are willing to opt out if they are given a chance to,[10] and there is growing pressure in the United States[11] and the European Union[12] to ban these practices across the board. This proves how the success or

9 Bowman, 'Why Data Interoperability Is Harder than It Looks: The Open Banking Experience', 5.

10 ArsTechnica, *96% of US users opt out of app tracking in iOS 14.5, analytics find*, at: https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/

11 Ban Surveillance Advertising, at: https://www.bansurveillanceadvertising.com/

12 Tracking-Free Ads Colation, at: https://trackingfreeads.eu/

failure of the UK "new pro-competition regime for digital markets" will depend on whether GDPR protections are retained or scrapped.

1.2 The interplay between data protection and the online safety bill

Open Rights Group do not believe that the Online Safety Bill will deliver on its objective to "keep the UK safe and secure online". Nevertheless, it is useful to emphasise the relationship between data-intensive business models and the occurrence of the harms that the OSB seek to address.

A driving force behind nowadays digital services is the so-called attention economy. Services rely on advertising for their financial sustainability and data-driven advertising requires an ever-growing amount of personal data to target individuals with personalised advertisement. In turn, platforms need increasingly sensationalist, polarising and emotionally-driven contents to increase engagement with their platforms, observe users' behaviours for a longer time, and draw inferences about their interests and characteristics. Evidence of this relationship is, for instance, Facebook recent decision to disable tweaks to their algorithm that prioritised authoritative journalism over click-baiting.[13] This decision was taken with the implicit but obvious intent of favouring the spread of incendiary contents to counter declining engagement.

The attention economy is in tension with the objective of "mak[ing] the UK the safest place in the world to be online", as well as with existing data protection rules that require as little data as possible to be collected and used in a way that meets individuals' rights and expectations. For instance, the Luxembourgish data protection authority recently issued a record fine on Amazon as they held that data-driven advertising is not necessary to provide Amazon's services.[14] A similar decision is expected to be taken by an Austrian Court against Facebook.[15]

These examples are revealing of two, opposite outcomes that UK digital regulations could achieve. On the one hand, the UK could retain existing data protection standards. Over time, advertisers would need to move to contextual advertising or other alternatives that do not require an ever-growing amount of personal

13 New York Times, *Facebook reverses postelection algorithm changes that boosted news from authoritative sources*, at: https://www.nytimes.com/2020/12/16/technology/facebook-reverses-postelection-algorithm-changes-that-boosted-news-from-authoritative-sources.html

14 La Quadrature du Net, *Amazon Fined 746 Million Euros Following Our Collective Legal Action*, at: https://www.laquadrature.net/en/2021/07/30/amazon-fined-746-million-euros-following-our-collective-legal-action/

15 NOYB, *BREAKING: Austrian Supreme Court asks CJEU if Facebook "undermines" the GDPR by confusing 'consent' with an alleged 'contract'*, at: https://noyb.eu/en/breaking-austrian-ogh-asks-cjeu-if-facebook-undermines-gdpr-2018

information. In turn, incentives for driving engagement at all costs would be reduced, and digital platforms would lose the incentive to fuel toxic dynamics.

On the other hand, the UK could go forward with their plans as outlined in “Data: a new direction”. This would allow digital platforms in the UK to rely on intensive data extraction and pervasive surveillance unapologetically. In turn, digital platforms would face even more pressure in dodging requirements imposed by the Online Safety Bill to protect their revenue streams. In turn, UK would be swimming against the tide, and would be bound to worsen rather than improve online safety.

2. How to achieve forward-looking and coherent outcomes in digital regulation

Retaining existing data protection standards would, in the long term, lead to market self-enforcement. If interoperability provides consumers with real choices, and platforms compete on products rather than data extraction, digital platforms will have to offer products that are private, secure, and valuable to their users.

Regulatory action will be a key driver to support the transition from the existing dysfunctional dynamics. In this regard, we take note of Government opinion that

"Regulatory interventions should address underlying drivers of harm rather than symptoms, in order to protect against future changes, and new regulations should be designed with a clear understanding of the links to our wider regulatory regime and goals".

ORG understands that this will lead to two main outcomes:

- stronger cooperation among Regulatory Authorities
- collaboration with businesses
- reliance on principle-based legislation, as opposed to prescriptive norms.

Open Rights Group believe that initiatives as the Digital Regulation Cooperation Forum constitute a rights step in this direction. As market failures in the digital sector usually engage with different fields (such as data protection and competition), Regulators will need to coordinate their efforts to ensure efficacy.

However, regulatory action is useful when it is effective and impactful. Therefore, "tak[ing] a collaborative approach through engagement with businesses" would undermine a Regulator ability to drive change in dysfunctional sectors, where market players are unwilling to change or to engage with authorities constructively.

Finally, Principle-based legislation has the benefit of being flexible and thus easily adaptable to change of circumstances or future developments. However, it also creates significant uncertainty over how principles should be applied in practice in a specific context. To address this issue, we emphasise the need to take stock of the failures by the Information Commissioner's Office to enforce in their remit effectively. Guidance and regulatory enforcement by the Authorities, as well as private enforcement and dispute resolution, are the avenues where principles find their practical application.

Based on ORG experience with the ICO, we identify three main areas where Government should consider intervention.

2.1 Making Regulators effective and decisive:

The Information Commissioner focused their first three years of regulatory action on nuisance calls and data breaches.[16] In other words, they have avoided dealing with difficult questions and systemic breaches of the law. For instance, a Report by the ICO determined that adtech practices are illegal in 2019,[17] but no action was taken to date. Another area of failure has been data brokerage, where years of investigation resulted in a rather mild enforcement notice being issued against Experian,[18] following their outright refusal to comply with basic data protection rules.

These experiences reveal how data-hungry businesses are unwilling to abide by the law, and preferred to game the ICO "constructive approach" by using industry engagement as an opportunity to buy time and avoid enforcement.[19] The ICO approach to regulatory action needs to become dissuasive against industry attempts to game the rules and dodge responsibility.

In this regard, we cannot but emphasise how changes being proposed in "data: a new direction" would worsen this situation. Tasking the ICO with duties that conflict with data protection will increase obstacles and barriers to decisive regulatory enforcement by the ICO. Duties to cooperate with other Regulatory Authorities and in the field of competition should be considered only and insofar they contribute to upholding data rights and promoting compliance. Other duties, such as

- "growth and innovation duty",
- "public safety duty",
- the duties to consider "a statement of strategic priorities" of the Secretary of State for Digital, and "government's wider international priorities".

are instead fundamentally incompatible with the oversight function of the ICO. It is particularly important that the ICO is not tasked with these duties.

16 Open Rights Group, *ICO enforcement overview – supporting data*, at: https://www.openrightsgroup.org/publications/ico-enforcement-overview-supporting-data/

17 ICO, *Blog: ICO Adtech update report published following industry engagement*, at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/

18 ICO, *ICO takes enforcement action against Experian after data broking investigation*, at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/

19 Open Rights Group, *Bringing sticks to a gunfight: how the ICO fails to enforce the law*, at: https://www.openrightsgroup.org/blog/bringing-sticks-to-a-gunfight-how-the-ico-fails-to-enforce-the-law/

2.2 Regulators must be held accountable by complainants:

The lack of effective avenues to challenge ICO decisions reduced the ICO effectiveness in their regulatory activities.

This is particularly evident in the field of adtech, where the ICO is still conducting an investigation but have closed the complaint initiated by Open Rights Group as a way to avoid scrutiny and accountability for their failure to act upon their findings. This approach was made possible by the Information Tribunal's interpretation to Section 166 of the Data Protection Act 2018, which admits challenges to the ICO on solely procedural grounds.[20]

Open Rights Group is challenging this interpretation in the Upper Tribunal,[21] but it ought to be stressed that this state of affair need be fixed regardless of the outcome of our legal action. Data subjects must be able to ask and obtain substantive recourse against ICO inaction via the Information Tribunal. Other measures to ensure that data subjects can hold the ICO accountable in the exercise of their discretion should also be considered where appropriate.

2.3 Private enforcement and collective redress as a second-line of defence:

Widespread illegality and market failures across digital markets resulted in significant pressure on Data Protection Authorities. It would be unrealistic to expect that DPAs alone can provide fully effective oversight to all activities involving personal data.

On the other hand, collective redress mechanisms have the potential to provide a suitable alternative to data subjects to obtain remedies against infringements. In order to be effective, both the ICO and collective redresses need to be functional, where:

the ICO would be better suited to address systemic issues and enforcement actions that are meant to promote compliance on the market or regulatory re-alignment;
Individuals would be empowered to seek redress in straightforward cases (like data breaches, nuisance calls, or infringements that affect individuals with similar interests), reducing the burden on the ICO to supervise day-to-day infringements that have little systemic relevance.

20 Upper Tribunal (Administrative Appeals Chamber) Scranage v Information Commissioner [2020] UKUT 196 (AAC), at: https://www.gov.uk/administrative-appeals-tribunal-decisions/scranage-v-information-commissioner-2020-ukut-196-aac

21 Open Rights Group, *Complaint against the AdTech industry body, the IAB, and Google in the Upper Tribunal*, at: https://www.openrightsgroup.org/press-releases/complaint-against-the-adtech-industry-body-the-iab-and-google-in-the-upper-tribunal/

The UK legal system already enshrines much of the tools that would be needed to empower individuals, consumers and public interest organisations to contribute to data protection enforcement. Article 80(2) of the UK GDPR could be implemented, thus allowing autonomous representative actions by public interest organisations. In the Civil Procedure Rules, the Lloyd vs. Google case could clarify the scope of CPR 19(6) by allowing collective opt-out actions.

Representative actions under the UK GDPR and collective opt-out actions under Civil Procedure Rules must be fully enabled. This would naturally lead to self-regulatory outcomes that result from consumers and businesses litigating and negotiating solutions without public intervention. On the other hand, Regulatory Authorities could invest their resources in those areas where the nature of ecosystems or the widespread nature of abuses requires top-down intervention. The same would be true in those areas where individuals may not be willing to come forward and expose their identities, either for being in a vulnerable position or for fear of stigma.

3. Conclusion

Evidence indicates that significant changes in the Government approach are needed to achieve a coherent approach to digital regulation. In particular:

- The notion of innovation needs to be rooted in human rights and promote individuals' agency;
- Existing data protection standards need to be retained, as doing otherwise would conflict with Government plans to promote competition in the digital space as well as online safety, and would ultimately undermine trust in the digital sector;
- The Government should abandon the notion of "business friendly" Regulatory Authorities, and focus instead on making regulators effective. Provide easy access to private enforcement and remedies would also foster self-regulatory outcomes without needing public intervention.