Written evidence from Horizon Digital Economy Research Institute, University of Nottingham (RTP0004)

1. Horizon[1] is a Research Institute at The University of Nottingham and a Research Hub within the RCUK Digital Economy programme[2]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley is Director of Horizon and was principal investigator on the ESRC funded CaSMa[3] project (Citizen-centric approaches to Social Media analysis) to promote ways for individuals to control their data and online privacy, the EPSRC funded UnBias[4] (Emancipating Users Against Algorithmic Biases for a Trusted Digital Economy) project for raising user awareness and agency when using algorithmic services and the EPSRC funded Defence Against Dark Artefacts project on the legal and technical security of Internet of Things. Dr Koene was a lead researcher of the CaSMa and UnBias projects, is Research co-Investigator on the EPSRC funded ReEnTrust[5] (Rebuilding and Enhancing Trust in Algorithms) project and chairs the working group for developing the IEEE P7003 Standard for Algorithm Bias Considerations. Dr Jiahong Chen is a Researcher Fellow of Horizon, working on the Defence Against Dark Artefacts project.

Questions

1. Are some uses of data by private companies so intrusive that states would be failing in their duty to protect human rights if they did not intervene?

- If so, what uses are too intrusive, and what rights are potentially at issue?

2. It has been commonly accepted that, under certain circumstances, States are liable for violations of human rights committed by private entities if the State concerned failed to fulfil its positive obligation to protect such rights. This is also confirmed by the case-law of international human rights courts, such as *Bărbulescu v Romania* (61496/08), where the ECtHR reiterates that States are under an obligation to ensure the use of personal data by private actors is subject to a legal framework that strikes a fair balance between competing interests.[6]
3. In this regard, the failure of a State to intervene in cases where there is a

[1] http://www.horizon.ac.uk
[2] https://epsrc.ukri.org/research/ourportfolio/themes/digitaleconomy/
[3] http://casma.wp.horizon.ac.uk
[4] http://unbias.wp.horizon.ac.uk
[5] https://ReEnTrust.org
[6] *Bărbulescu v. Romania* (application no. 61496/08), Para 127.

serious imbalance between the interests of private companies and the individuals to whom the data in question pertains could lead to a violation of human rights. A number of human rights that can be potentially breached in the context of use of data are listed below, exemplified with the latest instances of such breaches taking place within or outside the UK.

4. *Right to respect for private and family life (Article 8 ECHR)*
   In extreme cases where uses of data by private entities are highly intrusive, either due to the sensitivity of the data or the manipulativeness of the purposes, individuals are exposed to significantly high risks, which would entail States to take appropriate actions. For example, dating app Grindr has been reported to share HIV status data of the users to their advertising partners,[7] which, regardless of valid consent or not, is highly risky to the users as such data is of extremely sensitive nature. Another example is the online service The Spinner, who offers to influence individual behaviour by targeting them with personalised content enabled by cookies.[8] The private life of the individuals involved in both cases can be severely comprised and thus calls for interventions from State authorities.
5. A different form of impact of data driven technologies that constitutes a form of violate of the right to respect for private and family life, is posed by the intrusive nature of mobile apps that have been deliberately designed to trigger/reinforce compulsive behaviour (referred to as "stickiness" of interface design). As reported by many participants in our research studies with youths[9], the compulsive "stickiness" of many apps, including social media platforms, is causing disruptions of private and family life for large numbers (young) people in the UK[10].
6. *Prohibition of discrimination (Article 14 ECHR)*
   Use of data can also facilitate discriminatory business practices against protected groups of people. It has been revealed, for example, that Amazon has been developing an AI system to assist the recruitment process, which turns out to have significantly biased against female candidates.[11] Certain credit scoring systems are also found racially discriminatory, with the complex system taking into account behavioural or demographic data that is correlated with race.[12] What we consider no less noteworthy but often ignored is the discrimination against vulnerable

---

[7] https://www.bbc.co.uk/news/technology-43624328
[8] https://www.ft.com/content/944d068c-8a99-11e8-affd-da9960227309
[9] THE INTERNET ON OUR OWN TERMS: How Children and Young People Deliberated About Their Digital Rights
[10] Commons Science and Technology Committee "Impact of social media and screen-use on young people's health inquiry" submission SMH0131
[11] https://www.reuters.com/article/us-world-work-thairecruit/youre-hired-thai-startup-fills-gap-in-tech-talent-recruiting-idUSKCN1PM05D
[12] https://www.washingtonpost.com/business/2018/11/14/are-you-minority-borrower-you-might-want-think-twice-about-using-an-online-lender/

groups of people that are not explicitly listed as protected categories. Concerns are raised, for example, about gambling apps using location data to identify and target users who are more susceptible.[13]

7. *Freedom of expression (Article 10 ECHR) and right to free elections (Article 3 Protocol 1 ECHR)*
These two rights have long been recognised as closely related in particular in such cases as political campaigns and media coverage. The use of personal data may have profound implications for a democratic society and the related human rights. The ECtHR has repeatedly emphasised the importance of political pluralism and accordingly, States are under a positive obligation "to intervene in order to open up the media to different viewpoints".[14] While this is examined in the context of mass media, there is no compelling reason why this should not apply also to the online setting. The potential involvement of Cambridge Analytica in the EU Referendum[15] has clearly raised a number of issues surrounding political uses of personal data, notably the possible chilling effect on political debates, the unfair advantage gained by political campaigns, and the exacerbated social polarisation caused by political "filter bubbles".

2. Are consumers and individuals aware of how their data is being used, and do they have sufficient real choice to consent to this?

8. In the context of collection and analysis of personal data, individuals – especially internet users – are faced with a lack of real choice on various levels: First, many online service providers have made the provision of service conditional on the user's consent to the use of personal data. Second, some powerful players are so dominant in the market of certain sectors that individual users in effect have no alternative options. Third, the complex data network in the digital economy means that, even if a user may switch from one service to another, they might end in the same data network whose participants may continue to gather data from the same user, which is aggravated by the lack of transparency regarding the activities of such actors "behind the scenes". Fourth, the "free to use" business model based on monetisation of personal data can be so overwhelmingly prevalent in certain types of services that users have no effective choice but to gain access to such services by giving their data; while certain services allow users to opt out of being shown personalised adverts, that frequently does not stop the collection of data and amounts to an illusion of choice.

9. As part of our work with the 5Rights Foundation[16], we ran a series of

[13] https://www.telegraph.co.uk/news/2018/06/25/gambling-firms-could-use-gps-tempt-vulnerable-customers/
[14] *Communist Party of Russia and Others v. Russia* (application no. 29400/05), Para 126.
[15] https://www.theguardian.com/politics/2018/apr/14/leave-eu-arron-banks-new-question-referendum-funded-brexit-cambridge-analytica
[16] https://5rightsfoundation.com/

'Youth Juries'[17] workshops with young people aged 12-17, as part of the CaSMa and UnBias projects. During these workshops we delved deeply into how internet services really work, and participants discussed how they use the internet and what their concerns are. The Youth Juries included a large discussion of their experiences of the Terms and Conditions and user agreements of social media platforms. Participants explained that these were largely inaccessible. Whilst they shared their anxieties around the sharing and selling of their data by social media platforms to third party companies, or companies having access to their data, many pointed out that this was an inevitability if they wanted to use the app; *"yeah, because it's like things like Snapchat or Twitter, then you can do location or you can't download that app unless you agree to them accessing your location."* Others believed that there were not any other alternatives to them: *"But then you could argue there aren't really better alternatives, so you kind of have to let them use your data because there aren't many websites that will be willing to not use your data because it benefits them."* Many were resolute that they would accept these conditions regardless of what they involved as they wanted to be part of the platform: *"I kind of think well they're usually the same as most things, so if you read it once then there's no point in reading the other ones, but it's kind of like usually you're going to press OK anyway necessarily if you read it or not and it never really affects if I don't read it, because I'm obviously going to, if I read it and see something I don't like, I'm probably still going to say OK, I'm OK with this, so it's not necessarily…"*

10. Many Youth Juries participants were not aware that by agreeing to the online terms and conditions of social media applications, their data was being shared and sold to third party companies. Young people's main concern was around the data that they considered to be incredibly personal, such as their location data. Many were very uneasy that a social media company had the ability to track their location and share it with other third-party companies.

11. We also have great concerns regarding misleading terminology in privacy dashboards for selecting privacy settings within a platforms or apps. It is often not clear to users to what extent changing "sharing settings" from "public" to "friends only" or "private" affects the data collection by the platform or just the visibility to other users on of the platform.

12. As reported in the findings of the 'House of Commons Science and Technology Committee report on Responsible use of data'[18], and many subsequent investigations, there are grave concerns about the ethical

[17] https://uyj.wp.horizon.ac.uk/
[18] http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf

implications of standard practice around 'Terms & Conditions' (T&Cs) as means for gaining 'informed' consent from users for accessing and using their data. Much of these concerns is related to the length and difficult language used in the T&C documentation and the resulting habituation of people into 'click-signing' T&Cs without reading, let alone understanding, them.

13. The introduction of an "Age Appropriate Design Code" as part of the Data Protection Act 2018 represents a significant opportunity in this regard for establishing strong requirements on the understandability of T&Cs for the users of online services.

14. We note with concern however that efforts to produce a traffic-light style "kite-marks" type labelling scheme for a simple-to-understand communication of data-privacy levels of internet services has yet to show results despite having been called for in the House of Commons Science and Technology Committee report on Responsible Use of Data (Fourth Report of Session 2014-15) and reiterated by the House of Lords Select Committee on the European Union Internal Market Sub-Committee inquiry on Online Platforms and the EU Digital Single Market (2016).

15. The flow of information online is increasingly mediated by filtering and recommendation algorithms that select and rank the messages and news items presented to users. Although critical in shaping the online experience, these algorithms and their effects remain opaque to users. This lack of transparency has the potential to be abused for censorship or manipulation purposes. Without transparency it is very difficult to identify what kind of bias these systems put on the information flows that citizens are exposed to. Furthermore, the increasingly smooth interfaces and high rates of success in producing satisfying results can lead to an uncritical acceptance of the information that is given.

16. In order raise awareness regarding data collection and use by algorithmic online systems, the UnBias project has developed a "Fairness Toolkit"[19] including "Awareness Cards" for use in educational settings or peer-to-peer learning. The Awareness Cards have attracted favourable interest from experts at Unicef, UNESCO, EC (DG Connect), CNIL, and many third-sector organizations dedicated to human rights in the digital domain.

3. What regulation is necessary and proportionate to protect individual rights without interfering unduly with freedom to use and develop new technology?

17. GDPR and the Data Protection Act 2018 represent two significant

[19] UnBias "Fariness Toolkit", including "Awareness Cards" https://unbias.wp.horizon.ac.uk/fairness-toolkit/

new sets of privacy related data protection legislation, which will require a number of years to be fully tested and clarified through case law.

18. Beyond Personally Identifiable Data however there are a number of developments in data usage by digital technologies that warrant closer regulatory oversight:

19. If current trends continue, the Internet of Things is likely to become one of the largest problem areas for cybersecurity and for privacy. Far too often security and privacy concerns are given too low a priority in the design process, resulting in easily hackable IoT devices. Particularly concerning are the examples, including connected baby monitors, voice-controlled TVs and toy dolls (e.g. Hello Barbie), that continuously stream very personal video and audio information to data centres, often outside of the jurisdiction of the UK (and EU) data controllers. A worrying result in this space are the finding of a U. Michigan study which showed that people who buy "Smart Speakers" (e.g. Alexa, Google Now devices) expect and worry that the devices will collect data from private conversations but have resigned themselves to the idea that "big brother" type intrusions on their privacy have become inevitable[20].

20. The other key areas that will require increasing regulatory oversight is the use of algorithmic systems, including machine learning, to infer and predict information about people. The human rights that are most directly affected by this are prohibition of discrimination and the right to privacy.

21. A central challenge will be to define what rights people should have with regards to inferences (model predictions) that have been made about them, or about "people like them"?

22. What level of control (e.g. requirement for consent) should people have over inference processes, especially if the inference is based on shared traits between groups of people (e.g. genetic markers within families)?

4. If action is needed, how much can be done at national level, and how much needs international cooperation?

23. When it comes to effective regulatory measures at national and international levels, policymakers should take into account the relevant legal, economic, technological, and political constraints.

24. Under the current data protection regime, national legislation may impose additional restrictions on the use of personal data under certain circumstances, especially when sensitive data is involved.[21] However,

---

[20] Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers https://dl.acm.org/citation.cfm?id=3274371

cross-border data processing activities (by multinational organisations/corporations, for example) are subject to further international legal instruments and could be regulated more effectively within international legal frameworks.

25. Economic power is another important factor for determining the appropriate level at which regulatory initiatives are pursued. While UK-based, small- and medium-sized enterprises can be more effectively brought under the scrutiny of national authorities, it would be much more challenging to negotiate with larger companies based overseas, or take enforcement actions against them. Accordingly, policymakers should consider the size and structure of the market in question in the UK, and the potential impact on the economy before seeking national measures instead of international cooperation.

26. International coordinated regulation is required in order to have impact on large US based corporations which have emerged within the US's specific regulatory framework. In this regard the EU has been an important player, where the UK will be a minor voice unless it continues to coordinate and support EU action in this area.

27. A related consideration is the technological implementation and potential circumvention of regulatory measures. Technical requirements and standards can be more effectively enforced at national level where the UK may exercise practical jurisdiction over the entities involved. Like economic power, the technological power possessed by some dominant players means that certain solutions (such as the web browser-based ones) would be better achieved with multinational initiatives.

28. In cases where the commercial practices of data uses are of particular domestic interests or political sensitivity, national measures may be prioritised as such circumstances would provide a stronger political momentum or even public mandate for such measures.

5. To what extent do international human rights standards, such as the UN Guiding Principles on Business and Human Rights, have a role to play in preventing private companies from breaching individuals rights to privacy?

29. The UN Guiding Principles on Business and Human Rights are of significant relevance as they have set out a general and actionable framework for States and corporations to evaluate the compatibility of business practices with the international human rights standards. However, the Principles are fairly generic and not detailed enough to address issues arising specifically from the use of data.

---

[21] See, for example, Article 9(2)(a) and 9(4) GDPR.

30. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (updated in 2013) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, modernised as "Convention 108+" in 2018) have set out a more detailed and practical framework to identify, prevent and remedy potential breaches of privacy and related rights by private entities, as well as certain cooperative mechanisms for mutual assistance and multilateral actions. Yet, the OECD Guidelines are not legally binding on States or private entities, whereas Convention 108(+) needs national implementation by means of data protection laws such as GDPR and Data Protection Act 2018.

31. Therefore, while these international human rights standards are helpful in setting out the general regulatory context, additional work will be needed to give them practical effect. One particular area where national policymakers may play a significant role is human rights impact assessment (HRIA), as advocated by the Guiding Principles. This represents a valuable opportunity for policymakers to translate the HRIA framework into national requirements that are more specific and enforceable, and to integrate such requirements into existing impact assessment schemes, such as data protection impact assessment (DPIA), which are mandated by the GDPR,[22] and competition impact assessment (CIA). It should however be noted that HRIA should not be confined to the right to privacy, but also other relevant human rights as identified above.

30 January 2019

[22] Article 35 GDPR.