Response to the call for Evidence on

The right to privacy: digital data

Submitted by
Prof. Derek McAuley, Dr Piskopani Anna-Maria, Dr Virginia Portillo, Dr Helena Webb, Dr Hanne Wagner, Horizon Digital Economy Institute, University of Nottingham.

28 January 2022

1. The potential benefits, including to research, to effectively use and share data between and across Government, other public bodies, research institutions and commercial organisations, and the existing barriers to such data sharing

The potential benefits of appropriate data sharing to ongoing medical research, improving health care and controlling/preventing communicable diseases were acknowledged by the legislators of data protection law [1]. Thus, sharing of data for these purposes is lawful when necessary to achieve those purposes and under the appropriate safeguards. As ICO pointed out, there is a misconception that data protection law is a barrier to data sharing. The law enables organisations to share data in a way that is targeted, fair, proportionate and secure [2].

During the past two years, the digital transformation through health and care system as a response to the pandemic has demonstrated that data protection regulation is not a barrier to proportionate sharing of data. New patient-facing applications, virtual medical consultations and COVID-19 vaccination service was created in record time. Although there were emergent and shifting demands for large scale data sharing, the health care public bodies were able to respond without a need for the Government to reform the legislation.

In addition, health data were used for medical research purposes and its use contributed to scientists' understanding of the virus and its impact to patients. As previously said, there is no robust evidence that supports the claim that research-specific provisions in current data protection legislation creates barriers for researchers or causing confusion and hurting research and innovation in any material way [3]. Moreover, if legal obligations were removed, research community could encounter difficulties in terms of sustaining participation of data subjects in research activities and in protecting and promoting public trust in research. In the context of using health data, is well documented that citizens are reluctant to give consent to share health information and without enough information and safeguards they will withdraw or falsify their data [4]. Also see above sections 3 and 4.3.

[1] Recital 53 of UK GDPR, Article 9 of UK GPPR and Section 19 of DPA 2018.

[2] https://ico.org.uk/about-the-ico/consultations/dhsc-consultation-data-saves-lives-reshaping-health-and-social-care-with-data-draft/
[3] https://doi.org/10.25878/gsc1-vz67
[4] https://www.theguardian.com/society/2021/aug/22/nhs-data-grab-on-hold-as-millions-opt-out

2. **The extent to which data issues are appropriately addressed by the Government's National Data Strategy, its draft strategy, data saves lives: reshaping health and social care with data, and its consultation Data: a new direction**

In NDS, Government announced its intention to a radical transformation of the use and share of data and analysed several benefits in improving people's lives and boosting the UK economy. Less importance was given on the fact that lawful and responsible access, use and share of data by public and private bodies protects society from harm, builds public trust essential to constructive improvements to public services and digital products.

In our Response to Government's **NDS**, we set general principles that are crucial to planning and implementing government's data strategy [1]. More specifically, we pointed out that any collection, transformation, or use of data should have regard to the level of accuracy, up-to-dateness, relevance and representativeness of the dataset so as not to misused. We also argued that data-related requirements in legal frameworks currently in force, especially data protection law, should be upheld and enforced effectively. Guidance documents or discussions regarding ethical issues are supplementary to the legal obligations. We emphasized that public sector data, especially sensitive personal data, should only be made public where its security, provenance and accountability can be guaranteed. We also pointed out that the government should prioritise and support businesses and organisations that adopt technical models that derive results from data without exposing data subjects to potential risks as insecurity and privacy invasion. They can also achieve more innovative results. Horizon has been a pioneer for over a decade in developing decentralised "edge" computing models (see e.g., the Databox project).

Government's Strategy ***Data saves lives: reshaping health and social care with data*** also focused on benefits of data sharing as having more control of one's medical record, improving health care, facilitating the work of medical staff and medical research. At the same time, there is insufficient consideration of protecting patients' privacy and autonomy and insufficient description of how the sharing of data will work in practice.

Ensuring that everyone has easy access to health data can be beneficiary to citizens' health and social care. However, there are occasions where such access can cause harm. Par example when a physician considers that if their patient knows all the details of their medical condition this could deteriorate patient's therapy. This could also be the case of parents or guardians access children/teenagers/vulnerable persons' medical records without their explicit permission.

In order to facilitate the use of data in the health context, Governments' strategy argues that a new legal obligation to share anonymised data for health and social care purposes must be issued. As noted by ICO, the infrastructure must be able to carry out that statutory duty, to be able to align and implement the anonymisation standards [2]. The staff as well as the infrastructure should be able to assure both data security and availability. At the same time imposing a duty rather than informing the public about the benefits and privacy safeguards

can lead to lose public's trust and confidence. So, we propose that giving the public the option to volunteer as blood or organ donation for the public benefit seems more appropriate and effective.

As it has also been observed by ICO, the Government needs to be clear about the role of private companies in the landscape of personal health data records and international flows of data. Government also needs to define what sharing for wider purposes and wider partners means. As pointed out, it is a potential of benefit from data sharing but also there is a potential to result in risk to data subjects' rights and freedoms [3].

Furthermore, there is a lack of an explicit recognition of privacy by design and default approach in this strategy although there are best practices to refer to. Par example the use of databases as QResearch, a consolidated database derived from anonymised health records of over 35 million patients, for research purposes demonstrate that the use and reuse of public sector data can create public benefit while protecting patients' identity and without risking being illegally accessed. [4]. Applications such as Solid Health application can provide a decentralized way to record and manage a user's health and fitness activity. Platforms such as OpenSAFELY are secure and transparent and ways of analysing electronic health records data [5].

Lastly, government in **Data: a new direction** consultation, highlighted that there are elements of current data regime that create barriers to research and innovation. Some existing rules and guidance were characterised either too vague or overly prescriptive, thus potential reforms were proposed. In our Response, we highlighted that although there is a scope for clarification and improving of data protection legislation, Government's priority should be to support existing efforts of compliance with the legal regime, guidance and best practices, rather than removing the existing legal requirements [6]. As highlighted, the idea that innovation and data protection as well as research and data protection are in opposition creates a false dichotomy. If anything, data protection requirements should be viewed as prompts for innovative data processing system architectures and safeguards of responsible research. Also, we noted that the relaxation of privacy standards (especially the so-called prescriptive ones) could create legal uncertainty and jeopardise UK businesses and organisations' operation in EU markets and EU research networks [7].

[1] https://doi.org/10.17639/9M8B-9P34

[2] https://ico.org.uk/about-the-ico/consultations/dhsc-consultation-data-saves-lives-reshaping-health-and-social-care-with-data-draft/

[3] https://ico.org.uk/about-the-ico/consultations/dhsc-consultation-data-saves-lives-reshaping-health-and-social-care-with-data-draft/

[4] https://www.qresearch.org,https://www.qresearch.org/about/ethics-and confidentiality/

[5] https://www.opensafely.org/, https://solidproject.org/team

[6] https://doi.org/10.25878/gsc1-vz67

[7] Regarding the EU research network in biobanking sector see: Andelka M. Phillips and Tamara K. Hervey, Brexit and Biobanking: GDPR Perspectives in Santa Slokenberga, Olga Tzortzatou, Jane Reichel (eds), GDPR and Biobanking Individual Rights, Public Interest and Research Regulation Across Europe - Law, Governance and Technology Series 1st Edition 202, pp.145-183, p. 179. The negative impact of relaxation of privacy standards in research has also been observed by ICO: https://ico.org.uk/about-the-ico/consultations/department-for-digital-culture-media-sport-consultation-data-a-new-direction/

3. The ethics underpinning the use and sharing of individuals' data in health and care contexts

The use and sharing of data in health and care contexts raises ethical issues central to bioethics (confidentiality, respect for persons and individual autonomy) plus core concerns in data ethics (anonymity, privacy transparency). There can be tensions bringing the two together; for instance, the practice of informed consent - often used in bioethics – can be hard to apply in contexts involving large volumes of data, which may be reused over time. This is demonstrated in sections 4.1 and 4.2 below. Furthermore, in these contexts, privacy does not simply relate to the secure storage of data; there is also the potential for inferences to be drawn about individuals from the data they share.

Previous controversies have highlighted the problems that can arise from the sharing of data in health and care contexts. For instance, the collaboration between Deep Mind and the Royal Free London NHS Trust, which began in 2016 [1]. The Trust shared data about 1.6 million patients to aid development by Deep Mind of a clinician support app called Streams. After public complaints the ICO later launched an investigation and in 2017 criticised the Trust for its failure to adequately inform patients how their data would be used or seek their consent. The Information Commissioner stated that more transparency in the process of data sharing was needed and noted that "the price of innovation does not need to be the erosion of fundamental privacy rights".

As noted above, large scale data sharing has formed part of the UK government's response to the COVID-19 pandemic without a need for legislative reform. However, ethical (and legal) concerns have been raised over some aspects of the response. For instance, the government creation of a register of vulnerable citizens whose details can then be passed on to supermarkets is lawful under certain measures but has raised legitimate concerns over invasion of privacy. Noting these concerns, the ICO issued a reminder that the data shared must be handled responsibly by supermarkets and must not be retained for any longer than needed [2]. Another example relates to plans for the rapid development of symptom and contact tracing apps, as well as immunity passports. Such systems have the capacity to collect up large amounts of data, which may be of interest to many commercial as well as governmental organisations. It was argued by some experts [3] that such systems should have minimum safeguards *in addition* to those already set out in law in order to ensure good practice and maintain public trust – for instance by guaranteeing that data collected for an app or immunity certificate would not be shared outside the NHS. Research has also explored the potential for privacy preserving contact tracing systems [4]. In December 2021 the ICO and UK Health Security Agency confirmed agreed measures to strengthen the protection of individuals' personal data with the NHS Test and Trace programme [5]

As also noted above public trust in data sharing is low. YouGov polling conducted in 2017 [6] suggested that 71% of the UK population are happy to share their anonymised personal health data if it can provide community benefits. However, 70% do not approve of the data being handled by big tech companies, with only 13% saying they felt such companies could be trusted with this kind of data. Trust must be viewed as a further ethical issue since poor practice damages trust and good practice can foster it. Furthermore, to take steps that do not align with existing levels of public perception and trust could itself be viewed as unethical action.

[1] https://link.springer.com/article/10.1007/s12553-017-0179-1
[2]https://www.theguardian.com/business/2020/apr/07/uk-supermarkets-contacting-vulnerable-patients-must-delete-data-when-crisis-abates
[3] 10.31228/osf.io/yc6xu
[4] https://algorithmwatch.org/en/our-position-on-adms-and-the-fight-against-covid19/
[5]https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/12/ico-and-nhs-test-and-trace-agree-data-protection-improvements-following-consensual-audit/
[6]https://www.digitalhealth.net/2019/06/yougov-survey-reveals-willingness-for-patient-data-to-be-shared/

4. The extent to which appropriate safeguards and privacy are applied in the usage and sharing of individuals' data

As previously observed, the current legal framework has significantly improved the level of data protection in the UK and brought about a cultural change of treating personal data more seriously [1]. There is an ongoing effort of compliance with data protection principles and obligations supported by ICO guidance and UK institutes' research activities [2]. More specific legal and technical support in this direction can be achieved through transparency and accountability. More heightened transparency requirements for uses of data in public and private sectors, including, for example, record-keeping duties to document data provenance, algorithmic models and impact assessment can be imposed.
In that sense, the fact the Government's data save lives strategy commits the NHS to publish the first transparency statement setting out how health and care data has been used across the sector by 2022 is welcomed.
4.1 Children are a vulnerable group of citizens often ignored in the debate about personal data usage. Our findings from the UnBias [3] project indicate that children care about their personal data and its usage by online systems. Children's expressed concerns related to data privacy and data safeguarding issues, and they demanded clear information from services profiting from citizen's data [4] [5]. Children expressed their desire for more control, informed consent and choices regarding data sharing and selling, and what this should look like [6]. Research evidence from this study was provided to the ICO when drafting the Age Appropriate Design Code (The Code) [7]. The current challenge is for the regulators to ensure compliance to The Code.
4.2 Although children are the only group of people explicitly considered vulnerable in the GDPR [8], and special attention should be given to this age group to protect children's privacy online- as addressed by The Code, the ICO indicates: "individuals can be vulnerable where circumstances may restrict their ability to freely consent or to object to the processing of their personal data, or to understand its implications" [9]. In this context, and in addition to our findings on children, our findings from the ReEnTrust [10] project demonstrate that many young people (16-25s) and older adults (65s and over) are not fully aware of the consequences of data sharing and selling by organisations, being unable to make informed decisions to give consent for personal data usage and sharing. In line with the definition of vulnerability by the ICO mentioned above, our findings indicate that many young people and older adults are also vulnerable citizens in relation to personal data management by organisations. This is a major concern shared by children, young people and adults and one that negatively effects their experiences of, and trust in data use. These experiences could be

improved through steps by Government, public and private organisations to ensure individuals' data safeguarding mechanisms, provide meaningful data transparency and facilitate accessible means and choices for citizens granting informed consent (e.g., opt out choices).

4.3 In general, citizens need to be able to understand any safeguards applied. Only if they understand how their data is protected and can they judge whether these safeguards are appropriate, as insights from our study examining individuals' attitudes and understanding of the Covid 19 Test and Trace system shows [11] [12]. This is the basis for developing trust and support for any safeguarding measures. Citizens further want safeguard measures and verifications built into the system rather than being reliant on outside assurances of safety and privacy through third parties.

Citizen have also voiced the need to keep their data private and anonymous where possible, especially in social environments where leaking such information could lead to awkward, unfavourable and embarrassing situations as for example in the above-mentioned study, when being infected by the virus and spreading it without knowing and others learning about this.

Furthermore, citizens did not want their data to be given to third parties without their knowledge, representing both a distrust towards government and private companies and how and to what purpose citizens' data would be used for. This distrust was informed by previously actions of the government, which made it look untrustworthy in the eye of people. Participants considered it possible that their government-held private data could be given to third parties, especially big technology companies, without their knowledge or consent. This suggests that government should take actions to create trust and proof itself reliable in the way it treats citizen's information, before considering ways to share data with other organisations.

4.4 The right to data portability in the GDPR gives agency to the individual. Sharing citizens data without their consent – and appropriate information - seems against this notion. Concurrently, existing public services, such as transferring NHS data between different parts of the country, can still be difficult and often are a long, unautomated process. It could thus be argued that before citizens data is shared with third parties, existing services should aspire to be more portable. Regarding any safeguards applied to citizen's private and sensitive data, they should thus furthermore not limit citizens legitimate interests, such as making sure that their new GP practice is aware of their medical history. This stands in contrast to other, private business driven sectors, such as the comparatively uncomplicated process of moving current account banks through the UK's world leading Open Banking system, which could be used as a promising model to apply to UK health services [13].

[1] https://www.horizon.ac.uk/wp-content/uploads/2021/11/PDF-4.pdf

[2] For example recent data breaches in NHS have been reported and ICO pointed out the importance of implementing the existing law while providing guidance https://www.independent.co.uk/news/health/data-nhs-patient-breaches-privacy-b1877154.html

[3] https://unbias.wp.horizon.ac.uk/

[4] Elvira Perez Vallejos, Ansgar Koene, Virginia Portillo, Liz Dowthwaite, and Monica Cano. 2017. Young People's Policy Recommendations on Algorithm Fairness. In *WebSci '17 Proceedings of the 2017 ACM on Web Science Conference*, ACM, Troy, New York, USA, 247–251.

[5] Dowthwaite, Liz, Helen Creswick, Virginia Portillo, Jun Zhao, Menisha Patel, Elvira Perez, Ansgar Koene, and Marina Jirotka. 2020. '"It's Your Private Information. It's Your Life." Young People's Views

of Personal Data Use by Online Technologies'. In *IDC '20: Proceedings of the Interaction Design and Children Conference*, 121–34.
[6] Creswick, Helen, Liz Dowthwaite, Ansgar Koene, Vallejos Elvira Perez, Virginia Portillo, Monica Cano, and Christopher Woodard. 2019. '"… They Don't Really Listen to People": Young People's Concerns and Recommendations for Improving Online Experiences'. *Journal of Information, Communication and Ethics in Society* 17 (2): 167–82.
[7] https://doi.org/10.17639/71dc-r165
[8] Stanislaw Piasecki, Jiahong Chen, Complying with the GDPR when vulnerable people use smart devices, *International Data Privacy Law*, 2022;, ipac001, https://doi.org/10.1093/idpl/ipac001
[9]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/
[10] https://reentrust.org
[11] Joel Fischer, Liz Dowthwaite, Camilla Babbage, Hanne Wagner, Elena Nichele, Jeremie Clos, Pepita Barnard, Elvira Perez Vallejos, and Derek McAuley. "Understanding Trust and Public Acceptance of Digital Contact Tracing in the UK", presented at the TAS-RUSI Conference on Trustworthy Autonomous Systems, 30 June – 2 July 2021
[12] Dowthwaite, L., Fischer, J., Perez Vallejos, E., Portillo, V., Nichele, E., Goulden, M., & McAuley, D. (2021). Public Adoption and Trust in the Covid-19 Contact Tracing App in the UK: A survey study. *Journal of Medical Internet Research*. https://doi.org/10.2196/29085
[13] Stranieri, A., McInnes, A. N., Hashmi, M., & Sahama, T. (2021, February). Open Banking and Electronic Health Records. In *2021 Australasian Computer Science Week Multiconference* (pp. 1-4).

This submission was supported by the EPSRC Grant Number EP/T022493/1. 3
Any enquiries regarding this submission should be sent to: horizon@nottingham.ac.uk