Written evidence from Mavis Machirori, Stephanie Mulrine and Madeleine Murtagh, Policy Ethics and Life Sciences Research Centre (PEALS), Newcastle University (RTP0022)

We submit this response in a personal capacity. We draw upon our research about responsible and respectful data sharing and public engagement undertaken over the past two decades as well as experience in healthcare delivery and practice. We particularly reference research with members of the public about health data uses and governance undertaken as part of the Department of Health funded Connected Health Cities North East and North Cumbria project. Additionally, we incorporate personal perspectives gathered within clinical practice and wider aspects of social concern drawn from our personal backgrounds. Ms Machirori draws upon over 10 years of experience in working in health care, in which she has noticed changes in the use of personal data both within and outside of health practice, taking an interest in how changes noted within technology are projected onto African countries. Ms Mulrine has worked in research settings examining health inequalities for over a decade, and is particularly interested in health and social care practices that compound already existing injustices for marginalised groups in the North East of England. Prof Murtagh leads a programme of research examining and developing responsible and respectful sharing of health and research data in regional, national and international settings. We provide some insights related to the Terms of Reference which we hope the Committee will consider in its deliberations.

Our response focuses on Questions 1 and 2 of the Terms of Reference, with our response to Question 1 drawing on more specific examples, while Question 2 brings in different personal perspectives.

Question 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?

1. Authors of this submission conducted independent research in the North East and North Cumbria for the Connected Health Cities – NENC project to explore public perceptions about the digital sharing of health data through the Great North Care Record (GNCR)[1]. The research was undertaken collaboratively by Teesside University, Newcastle University and Healthwatch in 2017 and 2018. Public engagement and focus group sessions in multiple locations across

the region were undertaken with 314 members of the public. The findings suggested that most people would be concerned about their personal and sensitive health information, given for one purpose, being accessed by private companies for profit. Members of the public expressed concern about the potential of private companies, who seek profit and are largely unregulated with regard to health data uses, to use information in way which could marginalises or exploit vulnerable persons or populations. For example, if medical information was sold or shared to determine insurance claims or employment decisions, members of the public were very clear they would not want to their data used for such purposes. Concern was expressed about potentially intrusive uses of data to profile individuals or groups based on race, gender, mental health and socio-economic status. Members of the public worried such intrusive uses would be mismanaged and used to make public access to services or support more difficult. Focus group discussions referred to the stigma associated with mental health issues as an example of information that may not be relevant for others to know yet could lead to discriminatory profiling or treatment if shared with or accessed by private companies. The expectation of a right to a life free from discrimination was clear in the responses of members of the public in this research.

2. The GNCR Public Engagement research identified that members of the public regarded as acceptable the use of NHS-generated data direct care, service improvement and planning, and to a certain degree for research purposes[2, 3]. There was concern about private companies deriving profit from data generated and held by the NHS without an explicit public or institutional benefit. Sharing health data was understood as having a clear benefit for patients, the NHS and the wider society with research conducted by universities considered to be trustworthy while that related to commercial companies was not. The motives of private companies accessing health information were regarded with suspicion and not necessarily thought to be in the publics' interests. Members of the public expected to have control over how their information was used and by whom [4,5]. They viewed this as key to ensuring their privacy was maintained as the right to privacy was something they valued highly. Data sharing was therefore acceptable only in situations where a very clear public benefit was evident. The prospect of private companies being able to access data from an individual's

health record in the future, without their full knowledge or consent, was a threat that would erode trust between the individual and community and the Great North Care Record, or more broadly the NHS.

3. The pace of technological change is rapid and it can be labour intensive to keep up-to-date with the implications for one's privacy or digital footprint. There can be unintended or unanticipated consequences due to these privacy and technological changes. Whilst some may bring benefits for publics, patients and the NHS, it is important to be open to hearing and heeding the concerns of those affected, and to ensure those who are marginalised also have a say. The consensus from the focus groups was that reciprocity and agency were key to how they would shape their data sharing practices, but there was an understanding that the lived reality for many individuals meant that they spent a great deal of time trying to understand and make an informed decision on each and every change. This was not feasible for them. As technologies, processes and policies change, it was expected that these changes be communicated in a clear and timely manner. Where communication was effective and timely, it was judged that agency over personal health data would still have to remain in the hands of the individual.

4. Participants also reflected on the changing political landscape which could affect how their data was valued and how their data was protected. In order to safeguard against some of the risks outlined above and to give reassurance to members of the public our findings suggest that governance and oversight of any digitally enabled health data sharing should be formalised, authoritative and continuous. In order that this governance is fair and meaningful it should include the involvement of members of the public. Involving the public in decisions about governance and access to data will ensure their perspectives are respected and given legitimacy. Whilst this may not assuage the concerns of all, inclusion of publics in the governance process, including public oversight of private interests and data uses, is crucial.

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

1. One of the issues which must be considered is how 'data' and data use is defined and understood. Can we be sure that data is thought

of in the same way by all people involved? Those who send biological samples for consumer genetic testing may have very different expectations to those who provide data about exercise and diet on health-tracking mobile apps or are active participants in longitudinal or other health research.

2. There is a need to focus on how consent is collected. Consent is not a singular decision but a process which shifts and changes over time. Participants in the GNCR public engagement research expected that consent processes should have granularity – that is, be more than simple 'yes' or 'no' responses and be changeable over time and contexts. In relation to consenting, we ask that considerations be given to the ways individuals are able to track their personal information – or indeed when that information stops being theirs once they have handed it over to companies. While the Caldicott report makes the expectations of data transparency mandatory for health data, we would like to see these provisions extended to all data sharing and onward uses.

3. We have particular concerns about the health and social consequences of unregulated data mining, for example in maternity care. Maternity/pregnancy trackers which collate data about an unborn child such as the due date can be useful for mothers-to-be but can be used to target families with unwanted advertising. When those apps are populated with flawed or incomplete data, users are left vulnerable to potential misinformation and misuse of their data, including the resultant advice that is derived from these data. For example, incorrect data inputted in pregnancy trackers produces inaccurate advice to women – as identified by midwives working with Tommy's charity[6]. One's ability to enjoy the benefits of new technologies (which need people's data to be successful) is curtailed if that technology provides information that can lead to harm. But how can those who donate their data protect themselves and others against these harms?

4. It is concerning that information collected and stored about a pregnancy is not only used to market pregnancy and child-related products to the mother and her family but may provide personal information about families which is more insidious. A profile of the unborn baby created via ultrasounds may later be matched photos shared by proud parents of their growing children. These so called

'shadow profiles' are not new and have been identified as an issue within companies such as Facebook. These companies aggregate data about common characteristics from multiple individuals to create profiles of other, effectively collecting private data without people's knowledge or consent[7].

5. Data is relational and practices by UK publics have implications beyond UK boundaries. When digital data is aggregated or linked, we need to consider whether people within certain communities might become collectively associated with particular traits and negative ideas. Individuals are marked by digital data, even when they have not actively provided data, and can be subject to unfair decisions as a consequence. In this sense, those unwittingly linked lose their right to privacy through association and can potentially face discrimination by the digital footprints created around them. A real example would be access to personal contacts in one's online address book or phone contacts which are then used to create profiles about a person's unsuspecting contacts. The fact that these data links cross geographical boundaries is important, because people in low- and middle-income countries in the Global South for instance, will have data about them held by private companies which harness various personal or biometric data - but which are based in the Global North and the Far East and provide benefit mostly or only to those in power or who have access to this data. We ask that the Committee consider whether and how their inquiry might take into consideration how the rights of those connected-others could be protected. While this relational point speaks directly to the last point in paragraph 4 of Question 2, about shadow profiles, it opens the door to more sinister possibilities that biometric data is being used without people's consent or knowledge. This is demonstrated in recent media coverage of Artificial Intelligence facial recognition programmes in Zimbabwe and China[8] or concerns about Facebook's 10-year challenge[9], whether those concerns were founded or not.

6. A further concern relevant to this inquiry is whether and how consent can be meaningful and informed if people's data might be used in the future for purposes not currently anticipated or agreed to? When a participant agreed to broad consent in a research study they agree to unknown future uses but only with the reassurance that there will be appropriate governance of those uses. In relation

to data reuse more generally, we would question whether the structure of private companies are clear enough for the public to be able to differentiate one company as a whole from its subsidiaries or partners. As we have outlined in Question 1, members of the public have different reactions to data sharing dependent on the types of organisations involved. As the nexus between private and public entities is not always clear, such that even when public organisations collect data, that organisation's associations with private companies may remain hidden to those giving access to their data.

7. Finally, Human Rights such as those described in the call are currently unequal, if people have no say or knowledge of what those rights are. When people's data are shared outside of their geographical area without their awareness (as noted for instance in paragraph 5 regarding collection of facial recognition data in Zimbabwe by the Chinese company CloudWalk[10]) and when those people are already denied freedoms of expression, their rights are infringed. Additionally, data uses must be appropriate and proportionate, be it pregnancy, health or personal geospatial data or Artificial Intelligence decision algorithms. When AI is used to replace health and social care where there is otherwise little access, digital exclusion becomes discriminatory because only the already-connected can benefit from the technology and data use. The value placed on data will have unequal value for those providing the data (who may not see its value) and the private companies collecting and benefiting from access to that data. This creates unequal relationships between communities and commerce, health and industry. We believe the balancing of Human Rights should not be limited to personal data collection and storage, but must be placed in the context of other competing social and health needs, to ensure that privacy is not traded for other equally important rights and freedoms.

We are grateful that the Committee is taking time to consider this very important issue and we greatly appreciate your time in considering our contribution.

28 February 2018

References

1. https://www.greatnorthcarerecord.org.uk
2. https://www.greatnorthcarerecord.org.uk/information-for-patients/findings-workshop-sessions/
3. https://www.greatnorthcarerecord.org.uk/wp-content/uploads/2018/09/GNCR-public-engagement-report-FINAL.pdf
4. https://www.youtube.com/watch?v=uYuyfYOOM8I
5. https://www.youtube.com/watch?v=KOn9YBMrUo&list=PLPxAzdoCjqtBGWap8rL8H7ALvnh0g62_o&index=3
6. https://www.bellybelly.com.au/pregnancy/a-popular-pregnancy-app-spreads-dangerous-information/
7. http://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804
8. https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/
9. https://www.nytimes.com/2019/01/19/technology/facebook-ten-year-challenge.html
10. http://www.thezimbabwemail.com/technology-science/zimbabwe-imports-facial-id-technology-from-china/