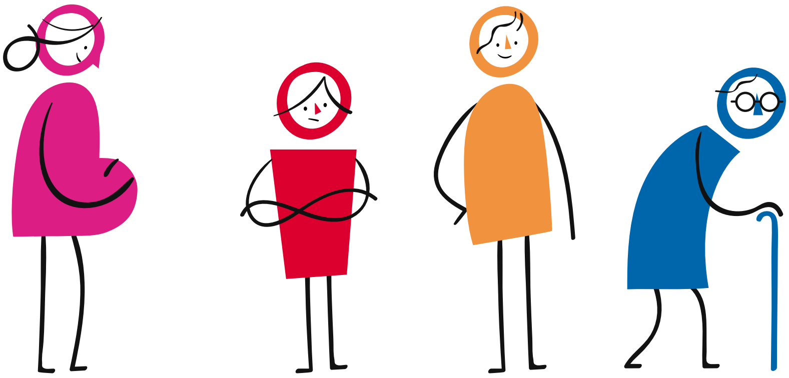
phg foundation
making science
work for health

My healthy future

discussion notes on privacy and autonomy



UNIVERSITY OF CAMBRIDGE

Roundtable on privacy and autonomy

Concerns exist that the implementation of personalised approaches to disease prediction, prevention and diagnosis coupled with digital technologies could compromise the privacy of individuals and undermine their autonomy.

The *My healthy future* roundtable on privacy and autonomy brought together experts from clinical medicine, health services research, law, history and philosophy of science and public health. Participants considered the impact that new technologies in healthcare could have on privacy and autonomy and how potential harms can be reduced and benefits increased.

The roundtable was held at King's College, Cambridge on 16 January 2019.

This document presents a summary of the discussion, which has fed into the *My Healthy Future* project and final report.

The views expressed are not necessarily those of the PHG Foundation.

Privacy

How to quantify privacy?

- Future health tech is often premised on high quality and high quantity of data
- Consequently, many of these new technologies may require us to hand over more data about ourselves than ever before
- However, does this mean that we have less privacy than before?
- How do we quantify privacy?
- This quantification point is important, as it may be true that we have less privacy but might also be true that we receive comparatively better care and treatment. Given this, the ratio of privacy loss to benefit ratio may remain the same
- We should consider not only what privacy is lost but also what we gain in return, in order to consider the ethical permissibility of this future health technology

Privacy as an investment

- Often the future of health technology is framed in terms of privacy loss and deprivation
- However, equally, health consumers may consider the privacy surrendered as an investment for better health technology
- Consequently, we should be aware of the normative framing we use to describe the use of personal data for health technology
- In some circumstances, it may be appropriate to see these interactions as transactions: health consumers pay with privacy and receive benefits in health technology. For example, access to health technology at a reduced or no cost
- Nevertheless, we should be wary of treating personal data as a mutually interchangeable (fungible) currency – often the disclosure of sensitive personal data may have far-reaching consequences, consequences not always made clear to the health consumer

Linked nature of data

- A single piece of information (a datum) does not exist in isolation; much of the value for health technology exists when datasets are linked together
- Many health technologies join existing datasets to generate novel conclusions. Further, many health technologies are set to utilise data not typically thought of as health data to generate conclusions about health. For instance, the Good Thinking project, where the digital footprints, from around 40,000 people are used to better understand and identify those people with mental health issues . This project is exploring the potential for data trails to be used to target the offer of and accredited tools (apps) for self-support
- The linked nature of data also has consequences for the identifiability of any given datum. We cannot examine the identifiability of any given datum in isolation but consider the context in which those data exist and the data that it might be combined with to identify data subjects
- We must also consider the future context in which data is currently being shared or made available. It is clear that, as more data becomes available, and the means of linking data improves, the risk of identification and privacy loss increases

Data and third parties

- A feature of the market for personal data is that third parties that did not collect the data often process this personal data. This feature should concern us for a number of reasons
- First, data subjects may be un or under-informed with regard to where their data is processed and what entities process this data
- Second, the passing of data between entities may often mean that there is not a clear and secure chain of custody to ensure that personal data is processed in a way that is consistent with a) the purposes for which it was collected and b) the restrictions that were originally agreed
- Third, if data is processed by third parties, consumers may have fewer legal remedies available to control the flow of their data. Further, once personal data has been released, it may be difficult to stop its spread
- It was noted that the GDPR may assist with many of these issues, furnishing data subjects with various rights that engage in some circumstances. For example, the rights to be informed, the right to access, the right to erasure, the right to explanation, and specific rights to be informed about further processing of their data

Digital literacy and clarity

- More often than not, in transactions of personal data the data subject and data controller are not on an equal footing
- Among many data subjects there is a lack of understanding of why their data has been collected, how this data may be used, and the remedies available to them
- There is also a tendency for privacy statements that contain much of this information to be dense and unreadable

- Further, there is also a tendency for the terms and conditions to be opaque and burdened with legal terminology
- In this context, it is difficult to see how meaningful consent to data processing (including collection of data) might occur
- Given this, if the future of health technology is to be premised on transparent processing of data, we will likely have to reconsider the purpose of privacy statements and ensure that at least these instruments are readable, informative, and accessible for a wide range of populations
- Again, we should note that the GDPR may assist in these matters. For instance, according to Article 5(1)(a) data must be processed for lawful, fair, and transparent purposes. Further, there are specific provisions that require information and communications with data subjects to be 'concise, transparent, intelligible and easily accessible form, using clear and plain language'
- Qualitative studies exploring how older people manage multi-morbidities suggest that people value digital health technologies to support self-management but transparency needs to be actively managed. Trials of multiple technologies for self-management in patients' homes enable thresholds to be set for triaging action from care givers. In systems of this type, the main beneficiary is the patient rather than the health professional
- Putting too much onus on individuals to take responsibility for their own health risks creating unfair expectations

When does sharing information become sensitive to the individual?

- Often the public are highly willing to share personal data for their personal care or for healthcare research with a clear public benefit
- However, this openness to share is fragile and there is an inflection point of 'ickiness' where individuals will no longer be willing to share their data if the data requested is too invasive
- Trust plays a large part in willingness to share personal data: often data subjects do not read the terms and conditions but simply trust that their data will be processed in appropriate ways
- As a consequence, this trust can be easily be eroded by wider societal developments and scandals in other sectors (see, for example, the case of Cambridge Analytica)
- Processing of data in the absence of trust can often lead to a deep feeling of violation
- These issues also co-exist with inequality – often low socioeconomic populations are less willing and more wary to share their data, in turn, they are also often underrepresented in datasets
- Another concern is that some individuals may be asked to share their data when there is no appreciable benefit for them and perhaps some risk of harm. It may sometimes be the case that individuals share data contrary to their own interests for the public good. This may be especially true if data is passed on to third parties such as insurers and so on
- Sometimes the inferences drawn from data will be important, rather than the facts themselves. It is less clear how standards might impact on inference generation or sharing

Might standards assist in securing privacy?

- In healthcare, we could make use of standards, seals, questionnaires and other methods to standardise data protection and provide assurances that data privacy and security are being protected
- There are around 300,000 health apps on the app library, many of which are poor quality. In a study of smoking cessation apps there was an inverse correlation between the quality of the app and how much it was used suggesting that there is 'no digital wisdom in the crowd'
- Regulation and standards could assist, for instance: NHS Digital’s Digital Assessment Questionnaire goes some way to protecting regulatory assessments and design principles and ensuring that a range of criteria have been met which carries an immediate trust benefit. Further, certain ISO (or similar) standards may also assist in ensuring that developers have the right processes in place to protect data subject privacy. Establishing a chain of custody for data could also be built into these or other regulatory frameworks

Autonomy

Shifting responsibility to the individual

- Does some of this future health technology shift responsibility for health from health systems to individuals?
- Are individuals adequately equipped to take on this increased responsibility?
- If the future of health is digital, a lack of understanding over how data is processed and a lack of digital literacy in general may mean that individuals are not well equipped to manage their own health
- There is likely a disparity between populations in their capacity to access health technology in terms of digital literacy, access to funds, and so on
- What will this shift mean for the social determinants of health?
- This shift in responsibility could be evidenced by a statement of informed consent from the user who consents to their data being used in a certain way. What are the limitations for informed consent?

What kind of choices does the health system want to provide?

- If personalised medicine is the future of healthcare, does this mean that individuals will have less choice over their healthcare?
- What kind of options should the health system provide? Could a proliferation of different choices lead to too much choice?
- There is no duty on health systems to fund suboptimal choices for individuals – generally, the most effective treatment (or cost effective) treatment is the one funded
- However, we should consider what kind of behaviours we encourage and discourage when funding health technology – are we funding healthy choices in the holistic sense of the word?

Are many of the findings generated actionable?

- Does future health technology generate clinically actionable findings?
- We should be careful about the unanticipated impacts of well-intentioned technology. For instance, overdiagnosis is a phenomenon that marks out those diagnoses that provide no clinical benefit but may induce significant psychological harm
- Do all populations have the capacity to act upon the findings of this technology? For instance, it may be cruel to attach a fitness tracker with constant nudges to exercise to a time-poor single parent with limited means. In short, the expectation that health technology will lead to behaviour change of individuals is simplistic if this fails to take account of the context and limitations that restrain users

Appropriateness of nudging

- Nudging modifies choice architecture to provoke behaviour change. However, nudging also raises distinct concerns
- First, do we pick nudging as the preferred behaviour change strategy for sound reasons? Cynically, this strategy may be relatively low cost and a modest proposal when compared with convincing health consumers via their rational capacities to change their behaviour
- Second, might nudging sometimes represents health consumers choosing the healthy ('right') behaviour for poor ('wrong') reasons? Does nudging always represent long-term healthy behaviour change or is its impact fleeting?
- Typically nudges are not tailored to the individual: broad based decontextualised nudges may be unhelpful and counterproductive in some circumstances
- Goal setting by the individual or health system can provide scaffolding for nudging behaviour over time
- One counterpoint: do we expect that behaviour change strategies must always encourage health consumers to pick healthy behaviours for good reasons? Might we be content with nudging in relation to some health behaviours? Might it be ethically permissible to nudge individuals to take the stairs instead of the lift, even if we recognise that this change does not represent a pure motivation toward health by the individuals?

Design

Might standards be part of the answer?

- A partial solution to standardise protections for health consumer autonomy and privacy might be the use of standards (e.g, ISO standards), seals, questionnaires, or curated libraries
- Of particular interest are ISO standards that incorporate certain privacy and security concerns, NHS Digital's Digital Assessment Questionnaire, and the NHS Digital Health App Library
- Perhaps we may learn from the use of accessibility guidelines, standards, and usability studies to make digital platforms more accessible for certain vulnerable groups e.g. disabled persons. Perhaps these methods might also help make health technology accessible to low socioeconomic status (SES) and elderly populations
- Standards and the like may be useful in encouraging excellence in access and usability for all populations. It may also help to ensure that the technologies and datasets are representative of the user population and not inherently biased either in development or operation. Standards might convert the good practice of the few to the baseline of the many

User centric design might be part of the answer

- User centric design is not a silver bullet to address inequality, privacy concerns, or autonomy concerns
- User centric design helps ensure that the device does what the user wants, ensuring the goal of the manufacturer and the end user has some overlap. However, user centric design does not secure respect for the end user's autonomy. Indeed, this method can simply be invoked to ensure that your product has a market to sell to
- In this regard, we should consider user centric design as a tool that can be used for virtuous or nefarious means. Consequently, while the tool is useful for usability, it must be invoked in the right context for the right reasons

Rethinking privacy policies

- Many confuse privacy policies with terms and conditions. We should sharply distinguish between these two instruments and acknowledge that they serve different purposes, and may be held to different standards. For instance, while both instruments usually serve a legal purpose, it may be easier to make privacy policies accessible since they exist to explain processing of data rather than as a part of a contract that may have to address many legal matters
- Nevertheless, privacy policies are often opaque, laden with legal jargon, and represent a tick box that secures legal compliance but little more
- The best privacy policies are simple, clear, and break down what data is collected, how it is collected, and for what purpose

- A rethink of privacy policies may be necessary, emphasising simplicity, accessibility, and compliance with the spirit of the exercise rather than another tick box
- Rethinking the temporal element might also be important, so that users have an ongoing privacy dialogue with service providers, possibly with input from an oversight body

Challenges complying with GDPR rights

- The GDPR furnishes data subjects with a number of rights: the rights to information, right to access, right to rectification; right to erasure, right to restrict processing, right to data portability, the right not to be subject to automated processing, and the right to explanation. However, it is important to note that many of these rights are not available to all data subjects by default – they are triggered only under certain circumstances and may/would not be engaged if the data controller relies upon certain legal bases
- The right to erasure (as well as the right to object) is a particular concern for health technology, especially machine learning. In some circumstances, the right may allow data subjects to demand that data controllers erase their personal data. Since machine learning models can be sensitive to small changes in their training data, this right may require that models be retrained post-erasure
- Despite the particular challenges associated with machine learning, it is important to avoid exceptionalist policy responses

Policy points

- Potential users of digital technologies will vary in expertise and capability. Vulnerable groups may need materials that are tailored to them to ensure that they are not excluded from the potential benefits associated with these technologies
- As technologies proliferate, the cumulative effect of multiple technologies is likely to lead to a highly complex picture of overlapping rights and responsibilities. In this scenario, secondary uses of data may make identification of data subjects more likely and privacy more difficult to protect
- Ideally, the design and development process should incorporate considerations of privacy and autonomy throughout, rather than retrospectively seeking to comply with applicable standards
- How to safeguard those people who opt out of using digital technologies completely, and ensure that they receive a satisfactory level of care?
- Even if data can be collected which indicates that a person is at risk, it is unclear when and how the health system should take action
- Personalised medicine could result in a restricted number of choices being available to individuals
- Taking forward policies to promote privacy or autonomy should be viewed within a wider political context in which sacrificing individual good might be regarded as being justified by a common good. Top down policy approaches might be needed to explore these cross-cutting political questions

Delegates

- Adam Kirk - Clinical Director at my mhealth and Consultant Physician
- Alessandra Pascale - Research Manager, IBM Research Ireland
- Alison Hall – Head of Humanities, PHG Foundation
- Chiara Garattini - Senior User Researcher, Public Health England
- Diarmaid Crean - Deputy Digital Director, Public Health England
- Hannah Murfet - Compliance Manager, Microsoft
- Hilary Burton – Consultant in Public Health, PHG Foundation
- Jeff Skopek - Lecturer in Medical Law, Ethics and Policy, University of Cambridge
- Jennifer Vance – Events and Engagement Manager, PHG Foundation
- Johan Ordish – Senior Policy Analyst, PHG Foundation
- Julie Doyle - Senior Research Fellow, Netwell CASALA
- Lukasz Piwek - Lecturer in Data Science, University of Bath
- Pashmina Cameron - Senior Research Software Engineer, Microsoft Research
- Sarah Cook - Policy Analyst, PHG Foundation
- Sybo Dijkstra - Head of Data Strategy and Artificial Intelligence, Philips
- Tanya Brigden – Policy Analyst, PHG Foundation

phg foundation
making science work for health

PHG Foundation
2 Worts Causeway
Cambridge
CB1 8RN

+44 (0) 1223 761900

www.phgfoundation.org

Contact: intelligence@phgfoundation.org