**Written evidence submitted by Dr Garfield Benjamin, Lecturer in Sociology, Solent University (DDA0036)**

## Introduction

I am a lecturer in sociology at Solent University, where I research the social impacts of technology, publishing on issues such as privacy, algorithms and AI, sociotechnical power structures, and online platforms. I also teach topics related to data and media, as well as politics. Solent University is an institution committed to access to education and a strong civic duty to serve the city of Southampton and the UK to be ready for the future.

Drawing on my recent research across a range of societal aspects and implications of technology, this evidence presents below a series of key themes and concerns that run throughout the proposals that are the subject of this call.

## Connected thinking for a connected society

While responses to issues of data and privacy need to be contextually aware and context-specific, the strategies and legislation concerning data cannot be siloed. Otherwise we risk establishing norms and expectations that are found (now or later) to contravene existing human rights or be otherwise harmful to individuals and society. For example, the previous consultation, Data: A New Direction, focused on Mission 2. This established a clear set of priorities within the broader strategy, making the government's agenda and political concerns very clear, along with highlighting equally clear risks of growth at the expense of justice and trust as an solvable problem (as discussed below). But each mission of the data strategy cannot be delivered on separately from the others. Similarly, these missions must be integrated with the foundations and opportunities - particularly those relating to responsibility and society, and a nuanced understanding of whose interests are being embedded in these notions.

I have elsewhere called for more cohesive regulation between privacy, data and online content,[1] and the same recommendations apply here. Greater emphasis should be made on bringing in not just the ICO and NCSC but regulators of wider social issues such as ECHR. This is essential to overcome barriers to administrative rights associated with data, particularly, for example, the specific need for greater power over one's data for trans communities (who have historically suffered administrative violence at the hands of state systems and data structures). While commitments such as interoperability and higher standards are admirable, it is essential that these rights and justice based issues are brought into the strategies and regulations before such standards are set. Similarly, a duty to share should not be legislated separately from enhanced duty of care - particularly over vulnerable or marginalised groups (such as children, vulnerable adults, or the trans community). Health and Social Care data should be held to higher standards than existing data protection legislation provides, with adequately resourced enforcement to ensure privacy is at the heart of the use of data.

---

[1] Benjamin, G. 2020. Digital Society: Regulating privacy and content online. Solent University. https://pure.solent.ac.uk/en/publications/digital-society-regulating-privacy-and-content-online

**Trust**

Trust appears as a key theme underpinning the proposals. But it is used in a way that seeks to extract or construct legitimacy rather than as a process of building relationships with those most affected. It often reads as though trust is expected, without recognising the power differences at work and the democratic legitimacy that requires a more nuanced understanding of trust (lessons we can learn from wider technology discourses but also from the problems of public communication and support for technical solutions to health and social issues raised during the Covid-19 pandemic). Trust must go alongside productive mistrust, for it is upon that balance that democratic processes rest. Trust cannot be solved, but nor can it be proxied as a measure of support without ongoing critical reflection. Trust must not be viewed as a metricised goal for adoption or legitimation of a certain project or use of data.[2]

Existing governance arrangements have made progress in recent years, but there are areas where improving the system will help to build trust by demonstrating more democratic principles. Foremost of these is independence of regulators and advisory boards such as ICO and CDEI. Within the context of more cohesive and connected arrangements, there must be space for critical perspectives. It is therefore important not only to engage with the full breadth of stakeholders (not simply different regulators, a handful of influential academic institutions and industry with vested interests). This should include wider perspectives that may interrogate government policy to ensure the commitments to privacy and other rights are upheld. Mechanisms can include broader engagement with more diverse academic, policy and advocacy groups, as well as more direct contact with those most at risk of harms through mechanisms such as citizen assemblies which have given voice and support to more far-reaching measures in issues like climate change. These arrangements are more likely to support privacy and ensure safeguards that are put in place are deemed appropriate by those who need them rather than by those who are not in need of such protections.

**Active privacy**

Privacy is not just something we have, it is something we do, and something we do together.[3] Our data is often not just about us, but about others as well: birth medical records are about parent and child; social care data likely includes information about family and relationships. Each time we share data or not, allow our data to be used or not, use data or not, we are making decisions for ourselves, for other people, and contributing to the norms and expectations of privacy in society. This extends from clicking accept on a cookie through to designing national strategies. The different contexts in which we 'do' privacy are important in building the broader understanding of what privacy is and what it means to different people. But this also means that not all privacy acts are equal. Some people's decisions about privacy shape the possible decisions of others. The design of systems and policies is a key area where the limits of norms are set, and how they are communicated to the public will influence the expectations people have and the possibility of debate or alternatives.

---

[2] Forthcoming text on trust and technology discourses.

[3] Benjamin, G. 2020. From Protecting to Performing Privacy. *Journal of sociotechnical Critique* 1(1) 1-30. https://doi.org/10.25779/erx9-hf24

The importance of language around privacy cannot be overstated. In the proposals in question, privacy is ill-defined, used only in a vague sense as a remote principle that will be sustained. The language on more concrete practices and systems focuses either on data protection or security and resilience. Each of these are important, but they are very different concepts from privacy, speaking to different sets of priorities. A much stronger commitment to privacy is needed in these proposals, as well as defining what that means for people. An active definition of privacy, mindful of context, would help here as it highlights the agency people can claim over their data and the impact of policies and systems on what privacy means for individuals and society. I strongly suggest a clearer definition of privacy and a firmer, more accountable commitment to those principles.

**Power and data**

Unlocking the power of data is really unlocking the power of people (as the data in question is about people, particularly in health and social care contexts). This highlights the inherent risks of exploitation in using data about people. It also raises issues of who has power in data usage and how this power is often masked by the terms we use.[4] Who is deciding how data should be used? And further than that, who is framing the questions? The government's call for evidence, and strategy, offers a very one-sided perspective emphasising economic potential and dismissing privacy concerns as being only from minority or fringe groups (we know this is not the case - see study referenced above) and solvable with data protection practices.

Unlocking the power of data must go alongside addressing the power surrounding data. This means learning from critical perspectives, listening to minoritised and marginalised groups, and giving meaningful voice to those who will be most affected by the uses of data (especially women, racialised minorities, LGBTQ+ and disabled communities). It also means, in practical terms, enhanced transparency about which private companies or research organisations will be involved in data collection, storing, processing or use. This information should be presented clearly and publicly in understandable terms, with adequate granular detail to help individuals trace where their data is going, be kept up to date with any new contracts or research projects. It should also include clear routes of consultation and/or redress on such government contracts, which would not only use the Information Governance Portal but may necessitate additional enforcement powers for regulators. This is particularly important in the commitment to support "up to 100 AI companies" where questions ranging from oversold technical capabilities to rights abuses surround data companies, and the terms under which they are being contracted (such as forward use of data beyond what patients might expect). Similarly, the commitment to fair returns in data partnerships is not adequate without a more equitable distribution of power surrounding the approval and audit of such partnerships.

**Critical skills**

Skills are critical to any digital strategy, and it is reassuring to see a substantial programme of digital skills for healthcare professionals embedded within the proposals. But these efforts

[4] Benjamin, G. (2021). What we do with data: a performative critique of data 'collection'. *Internet Policy Review* 10(4). https://doi.org/10.14763/2021.4.1588

must also include critical skills. Skills needs to include not only data use practices, not only data protection practices, but critical data practices. Essential skills include awareness of broader data ecosystems, how that fits into social power structures, and being able to make effective judgements about the way information is being presented about data use.

While the focus on health and social care professionals is admirable, the public must also be a focus of enhancing digital skills, particularly in the health and social care contexts which carry additional concerns. For example, specific aspects of health or social data might be considered quite differently from other information, and there is likely to be very varied responses from different people. An average response from someone who engages minimally with these services should not be taken as a benchmark. The focus should be on those most affected, and ensuring they are equipped with the skills to think about and enact privacy in a way that supports their situation and needs. A more comprehensive information campaign will be needed to make people how their data will be stored, shared and used, and by whom. Examples thus far, such as the linking of GP data for research purposes, have been conducted without adequate awareness. This particular case was also below standard by being opt-out. People need meaningful power over decisions about their data, and the awareness and skills they need is not simply to be able to manage this for themselves onf a practical level but also to be able to engage in decision-making about the use of data in society, especially when policy is setting new norms of acceptable uses for public interest. We must ask which public(s), and ensure those publics are able to make their voices heard before decisions are made, not just being able to dig through arduous privacy measures after the fact.

This thinking and approach to skills needs to extend to policy and policy-makers as well - as certain aspects risk misinforming the public and misrepresenting the privacy implications of the proposals. For example, the claims of anonymity are highly flawed. Particularly with health or social data, there is rarely such a thing as anonymous data. It is all too easy to de-anonymise such sensitive data. The phrase needs abandoning or qualifying. This is not only about transparency - what level or type of anonymity is provided - but also about clarity and setting appropriate safeguards in the form of expectations and norms that are adequately informed. What levels are people comfortable with? Do they understand the implications? Are policy-makers sure of the commitments they are making?

***January 2022***