POLICY BRIEF: Privacy

CODATA Data Ethics Working Group

Summary

- Privacy is a fundamental human right, and a requirement for individual and community wellbeing.
- However, privacy is also theoretically and practically contested and paradoxical.
- A critical understanding of privacy emphasises the importance of power and harm, and how this might differentially and contextually impact individuals and communities.
- Technological advance brings new categories of data, such as genomes, with which privacy rules need to be re-conceptualised and updated.
- For open science to maintain its values of quality and integrity, and collective benefit, we need to update how we conceptualise privacy, especially in the face of rapid and disruptive technological advancement.

Recommendations

- That open science explicitly adopt a more critical understanding of privacy that recognises underlying dynamics of harm and power that impact individuals and communities
- That the governance frameworks and policies for open science apply this more critical understanding of privacy/power in their deliberation and practice. This includes, but is not limited to:
    - Reconceptualising new data types (e.g. genomes) and their key terminologies (e.g. what is identifiability; what is personal, familial, and communal).
    - Developing governance policies and frameworks that are responsive and agile to privacy risks, harms, and power relationships as technologies advances.
    - Making data controllers and users to follow codes of conduct that are agreed upon by data providers and multidisciplinary stakeholders.
    - Investigating the appropriateness of restorative and reparative approaches where (potential) harms arise.
- That the training and development of open science professionals (such as data stewards) be provided opportunities to upskill in technical, social, legal, and political developments concerning privacy and related topics.

1. Introduction

The UNESCO Recommendation on Open Science (OS) notes privacy as one of several challenges and barriers for the implementation of OS. Indeed privacy can be a justifiable barrier and proportional restriction for OS. In others, it is listed as an emergent challenge for the implementation of OS amongst stakeholders. In both instances, privacy is mentioned vaguely, often without further development.

We argue that OS needs to consider privacy and its implications in greater detail in order to maintain its values and be successfully implemented. Despite common understandings, privacy is not an univocal concept. It is context-dependent and the rapid pace of technological development and disruption further complicates privacy. For these reasons, we encourage a more critical definition and usage of privacy in OS governance and policy, so that the values and principles of OS can be better maintained and enacted in the face of technical change and broader social challenges.

2. What is privacy?

Privacy is an interdisciplinary and diverse concept, ultimately describing relationships of exposure (Ball, 2009; Brighenti, 2007) or access (Anthony et al., 2017), and how much entities are exposed or accessible to other entities. For example, one classic definition of privacy by Westin (1970) described four kinds of privacy: solitude (freedom from being exposed or observed by others); intimacy (seclusion with intimate associates like family); anonymity (being invisible amongst groups of others); and reserve (restricted exposure to others). These four conditions describe different relationships of access and exposure, and show privacy is not a unitary concept, but contextually variable (Nissenbaum, 2004). What is exchanged (e.g. what kind of information is shared), how the exchange occurs (e.g. is it consensual), the expectations around how and where the exchange occurred (e.g. was there an expectation of exchange like in a public place), and other attributes can vary.

Privacy is critical for individual wellbeing, providing the basis for contemplation, personal autonomy, creativity, confiding and other psychologically behaviours necessary for a healthy life (Pedersen, 1997). Collectively, privacy provides the basis for autonomy, self-determination, and other social functions in society; protecting an entity from the unwanted interference or influence by commercial or political actors (Cohen, 2012b). It also plays a part in critical social processes of social cohesion, community, and compliance (Anthony et al., 2017).

While critical to many aspects of life, and recognised by nearly all as important, it is often paradoxical. The so-called “privacy paradox” (Barth & de Jong, 2017; Gerber et al., 2018), notes that despite being viewed as important by citizens, very few people engage in privacy preserving or enhancing behaviours. Instead acquiescence and disinterest dominate, despite evidence that citizens engage in complex “privacy calculus” (Kehr et al., 2015) discussions to think through issues around privacy. The exact reasons for this remain unknown. The privacy relationships is therefore one that is theoretically and practically complicated

3. **Privacy, harm, and power**

When rules or expectations around these contextual variables are broken - what Nissenbaum (2004) calls contextual integrity - then privacy harms results. As described by Calo (2011) privacy harms might include subjective harms (the perceived harm from a violation of these expectations such as embarrassment), or objective harms where exposure or access is used against an entity directly (such as selling or leaking personal data online). The ultimate root of this harms is a loss of control over the access/exposure relationships and aspects of this relationship – such as information about the entities in question or their attributes. This loss of control has been fundamental to how privacy has been conceptualised and practically addressed. For instance, some legal interpretations of privacy argue our information might be governed using the property law (Lessig, 2002), where defining personal information as a kind of property where ownership and exclusive control can support an individual's privacy. This also emphasises privacy as an individual right, rather than a collective or social contract (Cohen, 2012a).

Although control through property law is just one response to the challenges of privacy, it is useful to consider in the context of OS, given that it reveals challenges and limitations that are of direct relevance to OS. For instance, the social relations that are implied by property law (such as the rivalrous, mutual and exclusive ownership and usage of a specific object or asset) is not something that makes sense in OS. Data-sharing is essential for research, and cornerstone of the OS. Often, the data and very object study is shared in a way inconsistent with a form of property. In healthcare, for instance,the human genome is not necessarily individualistic because 99.9% is shared by all of us. In addition, it increases its utility as more genomes are shared and as technology advances (Box 1). Data here is both personal and public; a fundamentally different and qualitative original kind of data, with unique relationships and expectations that property law doesn't adequately cover. Property law is obviously not the only frame of reference or solution for privacy, but it is a useful starting point to acknowledge the existence of new categories of data that challenge how we understand privacy, its harms, and how we respond to them.

Box.1 Personal records maintained at public service sectors

Personal health records (PHRs) are usually managed at local hospitals and its personal identifiability or value (such as probability of contracting a severe disease) is often beyond the understanding of an average person. At the same time, sharing PHRs for better healthcare is an emerging issue in every nation. In England, National Health Service (NHS) is the tax-funded system that manages all kinds of health information from the primary to long-term care. In February 2016, NHS suddenly announced a partnership with Google DeepMind (later Google Health) to develop a monitoring application software for kidney diseases, called "Streams." The original plan was to develop AI to help general practitioners, or home doctors, to alert acute kidney injury. The agreement included access to data on 1.6 million individuals, including sensitive details such as abortion and HIV status. This deal ignited huge controversy over many issues around privacy and transparency. After much discussion, the agreement came to an end in March 2021 as originally scheduled,

and Google Health announced that it deleted all data it held. Streams service also ended simultaneously.

The intersection of personal records with private and identifiable information, and potential scientific use cases with private and public benefits, highlights the complicated nature of new forms of data and raises many questions relevant for OS. For instance, what are the kinds of acceptable scientific uses for this data (e.g. can PHRs be used for such short-term science projects or any pilot studies), and who owns the rights to use PHRs (do individuals retain control of PHRs given they have the potential to improve our healthcare as part of population level datasets and science)? Similar questions can also be raised in other situations where detailed, personally identifiable data is being collected, such as in education. Personal study records are often created and managed at the school level, and there is interest amongst governments to use statistical data for creating better education environment. However, who owns the right to use school data? Which education companies should be allowed access to the information and how? Such questions are not easily answered, and applying privacy, without a more nuance conception of the relationships and issues at stake, may not adequately address these challenges and opportunities, hampering the progress of OS.

This individual focus is an important issue for privacy, which we argue exposes how privacy is ultimately about power, which manifests certain kind of harms. We build off Marwick's (2022) observation that privacy is often unevenly distributed between different groups, with wealthy, male, and white individuals being far better represented in discussion on privacy than other groups. The harms of privacy are also unevenly distributed, with minority groups subject to greater privacy harms, but also social harms as a consequence of privacy violations (e.g. the loss of employment from having data leaked). Marwick's analysis demonstrates how privacy relationships are ultimately expressions of power relationships. Power is a social phenomenon concerning individual and collective control and conduct. A conceptualisation and emphasise on privacy as an individual right, or as a relationship where (an often socio-demographically privileged) individual is at the centre of everything ignores the broader context in which privacy sits, and how privacy *is* a kind of power relationships. A focus on broader contextual relationships is therefore essential to a holistic understanding of privacy.

This holistic understanding is essential in the context of rapid, disruptive, technological change - as we highlight above in Box 1. More data is being collected and utilised everyday in increasingly novel ways. From the capture of our data through internet services and mobile devices (Lyon, 2016) , to the use of sensors that can capture our faces (Andrejevic & Burdon, 2015; Gates, 2011), and other biometrics (Ceyhan, 2008), there are more and more relationships in which privacy is becoming a potential issue. Combine this with emergent abstractive uses of data (for a general outline see (Lee, 2021)), such as analytics that can predict personal psychological dispositions (McStay, 2020), or generative artificial intelligence that consumes the information humans create to imitate human like content (Dwivedi et al., 2023), a new set of privacy relationships is emerging. These relationships

will build upon, and potentially enhance existing privacy relationship issues, and potentially create qualitatively new ones as these and other unique technologies come to play.

Box 2. Biology specimens as community information

Even before the Human Genome Project in the late 20th century, biopsy specimens including personal genomes have been at the center of privacy discussion. The oldest immortal human cell clone, HeLa cells from Henrietta Lacks who died in 1951 for cervical cancer, has long been the standard laboratory cells in biochemistry and molecular biology. At that time, the rule of informed consent did not exist, and therefore, Lacks's family did not receive any credit resulting from the HeLa cell's extensive commercialization and societal benefits such as creating the polio vaccine. In 2010, a single book by Rebecca Skloot on Henrietta's fate changed the whole story. Now Henrietta's statue stands at the University of Bristol, the first user of HeLa cells, and her family is negotiating with multiple biotechnology companies for compensation.

Personal genomes are the digital equivalent of immortal HeLa cells. Personal genome is sharable and has a potential for medical advances including new vaccines and chemotherapy. It also contributes to defining genomic consensus of ethnic groups or nations for better healthcare. This advantage of collective benefits, however, may conflict with the privacy of personal information. Genomic sequence itself is not inherently person-identifiable, but with additional information such as genealogy, genomic data can be exploited to identify phenotypic characters including disease susceptibility. Once linked to other forms of data, it is possible that this data be is used to make judgements and assessments on an individual, that might have negative consequences (e.g. such as through risk assessments used in insurance). These concerns are compounded for vulnerable groups, such as those who are unwell, and those in marginalised demographic groups - such as people of colour. This is especially important, given Henrietta Lacks was an African American woman, and whose estate only recently received reparations for her mistreatment and unfair exploitation.

While science and the OS movement could see significant advances in scientific knowledge with greater sharing and use of personal genomes in healthcare settings, it also presents complex questions concerning the sharing of the identifiability of personal information. The current privacy rule such as General Data Protection Regulation (GDPR) are not compatible with such scientific nature on genetic data. The privacy rules mandate data erasure after consented utilisation, but each specimen including its digital information is a unique scientific record. For personal genomes, for example, accumulation for future utilisation is the standard protocol. A more nuanced perspective is therefore required.

4. Recommendations

Given the complexity and nuance of privacy, the OS movement and UNESCO's recommendation for OS face a number of challenges. First, the current definition of privacy does not capture the nuances of the concept, especially in light of new data types and relationships. The inequitable distribution of privacy harms necessitates a more holistic

conceptualisation of the power relationships and dynamics behind privacy, that is currently missing from the UNESCO OS recommendation. Current OS recommendation also do not engage with the qualitatively and quantitatively different kinds of data being created, that present unique power relationships and challenges (we used medical data as an example in this paper). Without more nuance in conceptualisation and terminology, associated privacy harms and issues cannot be addressed.

Without greater recognition and engagement with the unequal distribution of privacy harms (and benefits), and the power relationships behind them, core values of collective benefit, equity and fairness, and quality and integrity are also potentially undermined. Further to this, without recognition there can be no attempts at reparation and restoration. Given UNESCO's value of "collective benefit" through its science, there is an open question about how benefits and reparations might be made to those who are potentially harmed in the event of mistakes, or existing inequalities. The historical case of Henrietta Lacks (Truog et al., 2012; Box 2) is a testament to how science can be a source of injustice.

Access to data inevitably endows power on those whole control and manage access (who we might refer to as data controllers). When data originally come from individuals, e.g. personal genomes or school records, data controllers need to comply with certain codes that guarantee fairness and equality, and if necessary, equity and reparation if an individual or communities data has been exploited. To facilitate such codes, not only should data providers, users, and controllers be involved but also policymakers and technology developers for data management. Such multidisciplinary implementation has recently been explored in the idea of algorithmic reparations (Davis et al., 2021). Currently, the UNESCO recommendation is not engaged with this possibility.

Building on the potential limitations of privacy presently, and the need for multidisciplinary data management codes, there is an opportunity to nuance and improve governance and policy decisions under the OS framework. The need for these improvements is clear because of the relational nature of privacy and the emergent technologies connected to them. A static definition of privacy, and status quo approach to risk management and other governance activities will be ineffective in dealing with changes. A more agile and responsive approach is required to cope with the speed of change, and the variety of relationships at hand. While missing currently, there is an opportunity to improve the OS recommendation using this.

Finally, given the nuance and expertise required to engage with these topics, there is an opportunity to raise the profile of these issues to those working in the OS ecosystem, and support opportunities for their upskilling. Emergent and specialised data types and relationships require specialised knowledge and support, and there is an opportunity to connect OS professionals (e.g. data stewards and data custodians) with subject matter experts and learning materials to support them in addressing the challenges associated with new data types, or privacy in general.

Acknowledgements

The development and coordination of this policy brief was led by Lee Ashlin, Masanori Arita, Steve McEachern (Data Ethics Working Group , CODATA). We acknowledge and

appreciate the invaluable feedback on the policy brief by other members of the CODATA data ethics working group.

References

Andrejevic, M., & Burdon, M. (2015). Defining the Sensor Society. *Television and New Media*, *16*(1), 19–36.

Anthony, D., Campos-Castillo, C., & Horne, C. (2017). Toward a Sociology of Privacy. *Annual Review of Sociology*, *43*(1), 249–269. https://doi.org/10.1146/annurev-soc-060116-053643

Ball, K. (2009). Exposure. *Information, Communication & Society*, *12*(5), 639–657.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Brighenti, A. (2007). Visibility A Category for the Social Sciences. *Current Sociology*, *55*(3), 323–342.

Calo, M. R. (2011). The Boundaries of Privacy Harm. *INDIANA LAW JOURNAL*, *86*(3), 1132–1162.

Ceyhan, A. (2008). Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance & Society*, *5*(2). https://doi.org/10.24908/ss.v5i2.3430

Cohen, J. E. (2012a). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press.

Cohen, J. E. (2012b). What Privacy is For. *Harvard Law Review*, *126*, 1904.

Davis, J. L., Williams, A., & Yang, M. W. (2021). Algorithmic reparation. *Big Data & Society*, *8*(2), 205395172110448. https://doi.org/10.1177/20539517211044808

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., … Wright, R. (2023). Opinion Paper: “So what if ChatGPT wrote it?” Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, *71*, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York University Press.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Lee, A. (2021). Towards Informatic Personhood: Understanding contemporary subjects in a data-driven society. *Information, Communication & Society*, *24*(2), 167–182. https://doi.org/10.1080/1369118X.2019.1637446

Lessig, L. (2002). Privacy as property. *Social Research*, *69*(1), 247+.

Lyon, D. (2016). Big data surveillance: Snowden, everyday practices and digital futures. In *International Political Sociology* (pp. 268–285). Routledge.

Marwick, A. (2022). Privacy Without Power: What Privacy Research Can Learn from Surveillance Studies. *Surveillance & Society*, *20*(4), 397–405. https://doi.org/10.24908/ss.v20i4.16009

McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data & Society*, *7*(1), 205395172090438. https://doi.org/10.1177/2053951720904386

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(30), 119–139.

Pedersen, D. M. (1997). PSYCHOLOGICAL FUNCTIONS OF PRIVACY. *Journal of Environmental Psychology*, *17*(2), 147–156. https://doi.org/10.1006/jevp.1997.0049

Truog, R. D., Kesselheim, A. S., & Joffe, S. (2012). Paying Patients for Their Tissue: The Legacy of Henrietta Lacks. *Science*, *337*(6090), 37–38. https://doi.org/10.1126/science.1216888

Westin, A. (1970). *Privacy and Freedom*. Atheneum