Volume **3** (1) 2021 https://doi.org/10.5204/lthj.1924

Pulling Together or Pulling Apart: Opportunities for Privacy in a Pandemic?

[1]**Mark Taylor, Megan Richardson** and **Stacey Steele**
The University of Melbourne, Australia

Introduction: Pulling Together or Pulling Apart?

When we began writing this introduction, we were experiencing another strict lockdown in Melbourne, Australia. Coming to the end of our five-day forced quarantine, we were reminded of the end of our earlier 111 days of lockdown in 2020. At that time, we transitioned from physical restrictions on mobility to a more tenuous and contestable set of restrictions on privacy that impacted all levels of our everyday lives. To give just one example, when venturing into a cafe or restaurant after the 2020 lockdown, it soon became a familiar experience to be asked to provide a name and contact number for the purposes of 'contact tracing'. This process for identifying close and casual contacts of confirmed COVID-19 cases quickly evolved into a relatively sophisticated process, entailing a mix of QR codes, smartphones and digital platforms. However, it started naively. In the earliest days, the information was often captured on a piece of paper, attached to a clipboard and left somewhere prominent for patrons and visitors to take turns using—and even record for themselves, for instance, on their phones. The idea of writing one's name and telephone number on a piece of paper upon entry to a cafe or restaurant and then leaving it in a prominent place would have seemed absurd just 12 months earlier. Of course, not everyone complied, and there were complaints from contact tracers that occasionally people recorded the names 'Donald Duck' or 'Mickey Mouse' and gave false telephone numbers.[2] For those that did voluntarily comply truthfully, there may still have been a sense of 'privacy interference', however that might be understood (for example, because the information pertained to a sense of an interior private life, or simply because it concerned personal information about an identified or identifiable individual). The key question—at least among privacy scholars such as ourselves—was, could these processes be justified in the context of a global pandemic?

We introduce this special issue on Privacy and Pandemics by noting how difficult it is to answer definitively even the first half of this question: does asking people to write given name (family name was not legally required in Victoria) and telephone number on a piece of paper in a public space, and leaving that open to view and potential capture by others, constitute a *prima facie* interference with privacy? The answer to this question will likely turn on an interpretation of terms such as 'voluntary', 'public space' and 'private information' and the relevance of such terms to the operative idea of privacy and its individual and social importance.[3] Indeed, without contradiction, it is possible to hold more than one idea of 'privacy' simultaneously and perhaps answer the question differently from each perspective.

[1] This article reflects the authors' personal opinions. Statements do not represent the views or policies of employers, past or present, or any other organisation with which the authors are affiliated.
[2] Mark Saunokonoko, "'Mickey Mouse' Sign-ins Causing Problems for NSW Contact Tracers," *9News*, 21 December 2020, https://www.9news.com.au/national/coronavirus-turramurra-northern-beaches-hair-salon-victim-of-fake-sign-ins/6f8f96a6-8859-433c-abd1-9caac9c00ded
[3] Luke Cooper, "Coronavirus: Privacy Concerns Over Contact Tracing of Personal Details in Public Venues," *9News*, 19 July 2020, https://www.9news.com.au/national/coronavirus-australia-contact-tracing-personal-details-breach-risk-privacy-security-safety-covid19/9b7da004-f712-4346-9df2-55a47a79416d

If we move beyond instinctive assessments of privacy to consider privacy as a legal right, we might consider whether the practice constituted an interference with the right to privacy as defined by Australian or international law, for instance under the International Covenant on Civil and Political Rights (to which Australia is a party) or the Victorian *Charter of Human Rights and Responsibilities Act 2006* (subject to the Government's lawful exercise of its emergency powers). Questions might also be raised about compliance by certain businesses with the standards of the *Privacy Act 1988* (Cth) ('Privacy Act'). Alternatively, if privacy is viewed more broadly in terms of social norms, such as social constraints shaped by the normal practices and so-called expectations of a community even in the absence of formal law (or supplementing formal law), we might assess the practice against prevailing community norms. Such an assessment requires decisions such as whether the relevant comparator should be pre-COVID or embedded in the accepted practices during the pandemic as 'COVID normal' or some post-COVID reality. Alternatively, again, if privacy is viewed as something ethically grounded in notions of human dignity or liberal principles, then rational analysis may substitute for empirical assessment. Moreover, any such assessment is likely to be shaped, of course, by the assessor's disposition towards deontological or consequentialist ethics.[4]

Each of these high-level approaches can equally be extended to other prospective interferences with privacy that the COVID-19 context has entailed at various points over the course of the pandemic. They show that responses could be detailed and worked out in different ways. In each case, in the course of asking whether the practice constituted an interference with privacy, it would also be coherent to ask whether the practice was consistent with or contrary to the kinds of robust privacy protections that might reasonably be expected in a free and democratic society. At least some of those who gave accurate contact information may have done so because they considered it posed no unwarranted risk—that is, their assessments about legal and social norms protecting from the misuse of personal information may have been reassuring.

This observation leads us to our second point. Not only is it possible for multiple conceptions of privacy to operate simultaneously, and ground more *or less* consistent observations regarding privacy intrusion, but also—at least in some cases—privacy norms might be enabling, creating an environment in which people feel able to share data. An archetypal example of this is the doctor–patient relationship. Expectations of privacy can permit the free exchange of information between a doctor and patient that might otherwise be inhibited. Not all data flows are seen as posing serious risks to privacy;[5] some flows reflect the contribution that privacy can make to enabling a particular form of society. In such cases, the conceptualisation of privacy encompasses not only the keeping of information to oneself but also the free sharing of private information with trusted others.

The above points bring us to some deeper insights facilitated by the global pandemic. First, the urgency of crisis response has provoked rapid change—social, legal and regarding what may be considered ethically justified. Second, the rapidity of the change has greatly challenged the agility of institutions, systems and processes—which exist to protect privacy across each of these dimensions—to change together. There is a significant opportunity for legal privacy protection to create the conditions and space for valued human activity when different perspectives on privacy are in harmony and pull together rather than apart. For example, if the legal conception of privacy is out of step with social norms, this tension may undermine trust in governance. If legal or social norms cannot be ethically justified or identified, privacy protections may work against what is 'good' and what is 'right'.[6] When legal rights, social practices and ethical requirements work together, privacy protection may effectively propel society forward constructively: protecting the conditions necessary for human flourishing.[7] When any one of these elements is out of step, deleterious consequences for the others are likely, and the overall coherence of our data governance infrastructure is diminished. These insights are woven through the articles collected together in this special issue.

---

[4] For discussion of the distinction between deontological and consequentialist ethics see Larry Alexander and Michael Moore, "Deontological Ethics," *The Stanford Encyclopedia of Philosophy*, (Winter 2020), ed. Edward N. Zalta, https://plato.stanford.edu/archives/win2020/entries/ethics-deontological/

[5] For example, Alan Westin's position suggests that privacy 'is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.' Alan F Westin, *Privacy and Freedom* (New York: Athenum, 1967), 7. It is consistent with this idea of privacy that an interference with the ability to determine that information *is* communicated to others might constitute a privacy interference.

[6] For example, there is a feminist critique of privacy that recognises that privacy norms may shelter domestic violence. For reflection on this argument and a suggestion on how privacy might instead be conceived in a liberal democracy, see Anita L Allen, "Coercing Privacy," *William and Mary Law Review* 40, no. 3 (1999): 723–757.

[7] In relation to debates about data governance, a report by the Royal Society and British Academy noted that 'future concerns will likely relate to the freedom and capacity to create conditions in which we can flourish as individuals; governance will determine the social, political, legal and moral infrastructure that gives each person a sphere of protection through which they can explore who they are, with whom they want to relate and how they want to understand themselves, free from intrusion or limitation of choice'. The Royal Society and British Academy, *Connecting Debates on the Governance of Data and its Uses* (London: December 2016), 5.

Opportunities for Privacy in a Pandemic

The articles in this special issue illustrate a number of ways that the realities of a global pandemic may challenge different perspectives on privacy protection and the appropriate relationship with other rights and responsibilities. They arose from a virtual roundtable, held on 15 June 2020 at Melbourne Law School, under the aegis of the Privacy and Pandemics Information Network. The network was formed as a rapid response to the overwhelming number of privacy issues being raised almost simultaneously by, or as a result of, the various government and private actor attempts to deal with COVID-19 in Australia and around the world. Colleagues from different parts of Australia attended the roundtable, held via the ubiquitous means of 2020 communication, Zoom teleconference, and hosted and chaired by the editors of this special issue.

We briefly record the content of each paper as a reminder of the issues that were preoccupying us collectively at the time. Mark Burdon (Queensland University of Technology) considered 'Privacy Beyond the COVIDSafe App' and asked whether we should forgo information privacy law protections for COVID-19 mobile phone contact tracing. He has developed his answer to this question in an article co-authored with Brydon Wang and included as part of this special issue. Jonathan Liberman (University of Melbourne [UoM]) delivered a paper titled 'Testing, Testing, Testing', which discussed some of the questions raised by COVID-19 testing as a key pillar of strategies to move out of lockdown social and economic life. Alongside the government criteria for when a test is required and what a test result implies, he noted the—sometimes troubling—possibility of private actors (including employers and care home providers) developing their own requirements and responses. Mark Andrejevic (Monash University) continued the theme of interrogating the role of commercial organisations in the pandemic response with a paper titled 'When All Data is Health Data: The Role of Commercial Technology Platforms in (post) COVID-19 Health Monitoring'. Among other aspects, Andrejevic considered the role of companies such as Google, Apple and Amazon as they penetrate health sector infrastructure and sought to anticipate future tendencies in the post-COVID commercial datafication of health data.

The roundtable then shifted to consider data collection in more specific contexts. A paper jointly presented by Lisa Archbold (UoM) and Damian Clifford (Australian National University) titled 'COVID-19, Edtech, Privacy and Children' considered the impact of schools going online as part of the pandemic response. They compared the legal protection of students' digital privacy in Australia with the United States of America and the European Union. Their paper also has been developed into an article for this special issue; we discuss it further below. Ellie Rennie (Royal Melbourne Institute of Technology [RMIT]) and Stacey Steele (UoM) introduced another new perspective on the potential privacy impact of the pandemic response by considering the privacy implications of payment systems in emergencies. Again, the paper has been developed and included as part of this special issue.

Two more papers were delivered on the day. The first was presented by Marc Cheong (UoM) and Kobi Leins (UoM), titled 'Automated Decision Making by Government Agencies in Australia: The Tech, the Policy, the Ethics and the Regulation'. They considered the unintended consequences and risks of a technological response to a problem, particularly one presented as a technological panacea. Asking important questions about how automated decision-making (ADM) should be governed, they related more general issues with ADMs to the situation created by COVID-19. The last paper of the day was presented by Julian Thomas (RMIT). Titled 'Safety for Whom? Digital Citizenship, Inclusion and the Limits of Technological Solutions', this paper returned us to consideration of contact tracing apps and drew attention to the need to calculate costs and benefits of such apps with an understanding of the scale and social distribution of their likely use. Noting that COVID-19 is not an 'equal opportunity' pandemic, he encouraged better understanding of the impact that use, or non-use, of COVID-Safe or other contact tracing apps might have on already disadvantaged populations and the implications for them of issues including privacy, security and trust.

Inequality and inequity were themes picked up in different ways in most of the papers presented on the day and in much of the discussion that they provoked. There was a general consensus that COVID-19 and the response to it, by both government and private industry, raised crucial questions about how to determine what a 'fair' use of data looks like in a public health emergency and how to then govern against that standard. This observation returns us to our remarks about the significance of responses to a pandemic being able to prosecute normative agility *and* preserve (if not further promote) coherence with more than one idea of privacy. Legal change to facilitate uses of data with no breach of legal rights to privacy is inadequate if that change is insensate to ethical and social norms that are also adapting to the changed circumstances. Apart from anything else, it is unlikely

to enable data to flow in practice as readily as would normative synchronicity. Discord between perspectives undermines the opportunity that privacy protection offers to pull society together and enable valued activity.

The importance of normative synchronicity extends beyond simple perspectives on privacy to include broader perspectives and other values. For instance, in their article on 'Children's Privacy in Lockdown', Archbold et al. demonstrate the significance of incorporating reference to other children's rights—such as those relating to best interests and self-determination—when interpreting the scope of children's privacy. The authors raise questions about how adequately children's privacy was (and is) protected, as a matter of both law and practice, as schooling, play and socialising went online due to the pandemic. They observe that the impact of the resultant increase in surveillance has not been considered thoroughly, in part due to a historical failure to embed children's rights properly throughout decision-making processes, and argue that proper respect for children's privacy cannot be manifest simply by deference to parent decision-making. Rather, there is a need for *all* parties associated with children in the online environment to have some responsibility for what happens to them: parents, schools, software and system architects and platform providers, in addition to regulators and children themselves. As it is, privacy was not the top priority for schools responding to the pandemic, with issues of cost and available resources often motivating reliance upon 'free' applications. This focus resulted in 'vast amounts of user or behavioural data' being transferred to commercial actors despite the governance over this data being inadequate. The result was that children were left vulnerable to future uses of data in education and employment contexts. A failure to coherently integrate children's rights thinking into fundamental change for many children resulted in an insufficiently rich understanding of what privacy protection required.

The lack of agility of systems and regulation needed to respond efficiently and comprehensively to the pandemic is also taken up in Rennie and Steele's article on 'Privacy and Emergency Payments in a Pandemic.' They make several points complementary to the analysis provided by Archbold et al. while tackling a very different issue. In discussing the challenges of providing emergency payments to citizens during the pandemic, Rennie and Steele note again how *the response* to the pandemic, driven by the urgent needs of crisis response, may be inadequate. In this case, they show how a potential response to the logistical and administrative challenges in making emergency payments to citizens, revealed by the pandemic, gives rise to certain privacy risks. Focusing on one potential response, in the form of a central bank digital currency (CBDC), they describe four distinct privacy losses that might follow from current and proposed CBDC models: loss of anonymity, loss of liberty, loss of individual control and loss of regulatory control. As with children's personal data, as discussed by Archbold et al., a key concern is what happens next with the data incidentally collected as human activity is rapidly captured in the digital space. Much like the data collected about children online, they note the risks associated with downstream secondary uses; however, this time, the risks are of a different kind of inequality.

Conflating and Integrating Legal, Ethical and Social Norms

Thus, we return to our opening remarks about the value of being able to adopt an approach to privacy protection that is coherent in respecting privacy across more than one dimension: that is, not only treating the legal standards as separate and distinct from ethical and social standards around privacy protection but also finding ways to integrate the standards in a harmonious way. The importance of being able to do that through regulatory means that are consistent with social and ethical expectations as engendered by political rhetoric is taken up in the arguments of Burdon and Wang in their article on 'Implementing COVIDSafe'. They contend that the regulatory rationality for the legal protections contained within Australian COVIDSafe legislation was out of step with the rhetorical campaigning around the use of the COVIDSafe App by the Australian federal government. They argue that the dissonance between regulatory rationale and campaigning rhetoric was both a missed opportunity and a mistake if the aim is to promote public trust and confidence.

The COVIDSafe App was the smartphone application promoted by the federal government to provide a digital means of contact tracing. To promote use of the application, the government introduced the 'COVIDSafe legislation' to govern the data generated through the process underpinned by the application. Burdon and Wang argue that the data governance controls contained within the legislation strengthened the largely processual protections already contained in the logic and application of Australian data privacy law; they take the Privacy Act regime as the worked example of such law. These controls are primarily concerned with well-accepted principles of data protection (or data privacy, as it is more often termed in Australia), including accuracy, purpose limitation, data minimisation, security, transparency and individual control. By contrast, the rhetorical campaigning focused firmly on the moral duty to others, with downloading and using the app characterised as 'the right thing to do' and failure to download the app as 'un-Australian'.

Burdon and Wang argue that the COVIDSafe App regulatory framework introduced in the 2020 *Privacy Amendment (Public Health Contact Information) Act* was a missed opportunity to give substantive content to the Australian data privacy law requirement that data be processed fairly. By more clearly aligning legal and ethical requirements, the Commonwealth Government might have thickened the conception of unfair processing that inheres in Australian privacy law and more clearly signalled the requirement of benevolent intent. Such an outcome could have enhanced existing legal protections as a basis for guaranteeing equitable treatment. The ethical demands of the pandemic response provided an opportunity to articulate reciprocal responsibilities in a moral community and have data privacy law expressly work to support them—the ideal aim being to establish a value consensus, which, as previously described by Mayer et al., requires ability, integrity *and* benevolence on both sides, and is then reflected within the legal protection.

Burdon and Wang emphasise the opportunity that the pandemic represented to strengthen privacy protection in Australia while simultaneously enabling the necessary public health response. For the data to flow in ways that public health professionals require, there must be 'value congruence' and associated confidence that data will be used in ways that are legally, socially and ethically acceptable. The system of privacy protection must be sufficiently agile that it can pivot across any one of these dimensions without leaving the others behind. Likewise, as Ellie and Steele note in their paper, the changes that follow responses to the pandemic may result in a challenge to our traditional image of what it means to have privacy. However, that outcome does not mean that our image of privacy is diluted or undermined.

The image of privacy can change in ways that contribute to pulling society together by enabling and protecting activity in ways that the pandemic has prompted. Our understandings of the distinction between what is public and what is private may need to cut across our range of human activity in different ways, as we conduct online business meetings from our bedrooms and see our family computers shared with our children (and their cat filters). Finally, Archbold et al. make a call for us to expressly recognise that 'public' does not equate with 'not private'; there may be privacy expectations regarding data that is shared publicly and, they note, 'young people often find their private space outside the home'. As private space may be found outside, so are we making more public the spaces inside our homes, as we invite relative strangers in—and our children do the same—through the blending of the digital and physical infrastructure of our lives.

Conclusion: What About the Name and Number on the Clipboard?

Does the collection of data on sheets on clipboards then interfere with privacy? Perhaps, it is not just a matter of being required to give up private and personal data. If one holds a particular expansive understanding of privacy—as may be associated at times with the United States Supreme Court or, albeit to a slightly lesser extent, the European Court of Human Rights (or the Court of Justice of the European Union, for that matter) and is supported by articles in this collection—*enabling* individuals to meet and associate in cafes and restaurants is supportive of privacy (in the sense of fostering private relations and exchanges), and practices that serve to undermine that are doubly harmful to privacy. However, the legal controls on the processing of data needed to support such activity must be sufficiently robust to meet in fact—and not just in hope—the requirements of trustworthy governance, whether by governments or by business enterprises or, indeed, by powerful individuals.

As the experience in Australia suggests, if there is a lack of value congruence across each of the dimensions of privacy, and if the legal conception of privacy is out of step with social norms in fact or what is perceived to be a reasonable expectation in ethical terms, a lack of trust in government and business systems emerges. While a rapid response to a public health crisis is to be expected and welcomed, there exist dangers if it sacrifices the possibility of value congruence across each of these important normative perspectives. Such an outcome suggests a lost opportunity for conceptions of privacy, just when we become crucially dependant on the collective ability to gather and process accurate data (being literally, for some, a matter of life and death), and means that we are all the losers.