Volume **5** (2) 2023 https://doi.org/10.5204/lthj.2928

Contact-Tracing Technologies and the Problem of Trust—Framing a Right of Social Dialogue for an Impact Assessment Process in Pandemic Times

Rachelle Bosua
Open University of the Netherlands, Netherlands
Damian Clifford
The Australian National University, Australia
Megan Richardson
The University of Melbourne, Australia

Abstract

While technologies offer potentially powerful tools to help address complex social challenges, experience shows that they may fail to meet expectations and may also raise challenges of their own, including for privacy and other data rights. To what extent can these difficulties be ascribed to a lack of public trust undermining the technologies' effectiveness and disputing their legitimacy? The Australian and Dutch pandemic contact-tracing apps considered in this article suggest part of an answer to this question. As our case studies show, the greater efforts made by the Dutch Government to address a range of rights and provide for wide consultation in the CoronaMelder app's various impact assessments paid off in terms of a better-designed app that was more broadly conversant with human rights than its Australian COVIDSafe counterpart, and was also more trusted—even if these benefits were still marginal compared to manual contact-tracking, especially in already marginalised communities. We argue that the Dutch experience should now be taken further to frame a right of social dialogue allowing data rights subjects to participate fully in the impact assessment process. We hope (and expect) this would result in better decision-making and improved public trust in 'truly trustworthy' technologies developed and deployed in response to a pandemic. However, ultimately, our more basic argument is that rights, premised on dignity and liberty, are of value and should be respected, including—indeed especially—in pandemic times.

***Keywords**:* Contact-tracing technologies; impact assessments; pandemics; privacy; data; trust; human rights.

1. Introduction

While technologies offer potentially powerful tools to help address complex social challenges, experience shows that they may fail to meet expectations and may also raise challenges of their own, including for privacy and other data rights. To what extent can these difficulties be ascribed to a lack of public trust undermining the technologies' effectiveness and disputing their legitimacy? The Australian and Dutch pandemic contact-tracing apps considered in this article suggest part of an answer to this question. As we explain below, the case studies were selected inter alia because of the very different treatment of human rights in the Netherlands and Australia, despite other similarities, for instance, in terms of development and commitments to democracy.[1] In particular, the Netherlands is bound by the Charter of Fundamental Rights, which forms part of the constitutional

[1] Silver, "Smartphone Ownership"; OECD, Building Trust to Reinforce Democracy.

law of the European Union (EU),[2] and is a signatory member of the European Convention on Human Rights.[3] Meanwhile, Australia largely relies on formal adherence to international rights instruments such as the International Covenant on Civil and Political Rights.[4] As our case studies show, the greater efforts made by the Dutch Government to address a range of rights and provide for wide consultation in the CoronaMelder app's various impact assessments paid off in terms of a better-designed app that was more broadly conversant with human rights than its Australian COVIDSafe counterpart, and was also more trusted—even if these benefits were still marginal compared to manual contact-tracking, especially in already marginalised communities. We argue that the Dutch experience should now be taken further to frame a right of social dialogue allowing data rights subjects to participate fully in the impact assessment process. We hope (and expect) this would result in better decision-making and improved public trust in 'truly trustworthy' technologies developed and deployed in response to a pandemic.[5] However, ultimately our more basic argument is that rights premised on dignity and liberty are of value and should be respected. In short, respect for human rights should be not only an end goal but part of the process leading up to that end, including—indeed especially—in pandemic times.

2. Contact Tracing Meets Impact Assessment

As Karen Yeung and Lee Bygrave point out,[6] providing impact assessments as a way of addressing risks associated with the deployment of novel technologies is one marker of a 'modern' data protection regime that functions as a progressive instrument of regulation. An example is art. 35(1) of the EU General Data Protection Regulation 2016 (GDPR),[7] which states that:

> Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The terms of the impact assessment process are prescribed in the rest of the article—including making provision for public participation in the process in art. 35(9), which specifies that:

> Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

The GDPR process offers an example of a regulatory mechanism that aims to identify and mitigate potential risks, fairly balance with prospective benefits and, at the same time, provide for clear public accountability.[8] Yet, in practice, assessments often tend to be dealt with in a rather narrow technical or legal compliance-oriented manner,[9] with their focus more on the procedural analysis and risk management dimensions of the GDPR rather than engaging in forensic discussions of the GDPR's safeguarded rights and freedoms, which are instead left to data protection authorities and courts to elaborate.[10] As to the scope for public participation provided for in art. 35(9), the Article 29 Working Party, in its 2017 guidance, stressed that consultation need not occur in every case.[11] Even so, the combined emphasis on rights and public accountability in the GDPR provisions, as well as the Charter (and more generally the Convention), clearly informed the Dutch Government's conduct in framing and deploying its impact assessments in the process of rolling out its CoronaMelder app in the challenging environment of pandemic technologies being pitted against publics' concerns about privacy and data protection along with other rights and freedoms.

By contrast, Australia, with its more limited experience of human rights and impact assessments, was less well-prepared when it came to conducting an impact assessment for its COVIDSafe app under the emergency conditions of the pandemic. Although the International Covenant on Civil and Political Rights is mentioned in the preamble to the *Privacy Act 1988* (Cth), that is as far as it goes. And minimal provision is made for impact assessments in § 33D(1) of the Act, stating that:

[2] EU, "Charter of Fundamental Rights of the European Union 2012/C 326/02."
[3] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms.
[4] United Nations General Assembly, "International Covenant on Civil and Political Rights."
[5] Cf. Mantelero, Beyond Data, 82, and further below Part 3.
[6] Yeung, "Demystifying the Modernized."
[7] Special Eurobarometer 487a, The General Data Protection Regulation.
[8] Kosta, "Article 35 Data Protection Impact Assessment"; Kasirzadeh, "Fairness and Data Protection Impact Assessments."
[9] Kaminski, "Binary Governance"; Kaminski, "Algorithmic Impact Assessments Under the GDPR"; Mantelero, Beyond Data.
[10] Mantelero, Beyond Data, 21–22.
[11] Article 29 Working Party, Guidelines Data, 15.

> If:
>
> a) an agency proposes to engage in an activity or function involving the handling of personal information about individuals; and
> b) the Commissioner considers that the activity or function might have a significant impact on the privacy of individuals;
>
> the Commissioner may, in writing, direct the agency to give the Commissioner, within a specified period, a privacy impact assessment about the activity or function.

It is clear from the terms of § 33D that the Act's focus here is limited to government agencies, and the requirement for, as well as the nature and scope of, an assessment is left to the discretion of the Commissioner. For instance, the Commissioner, in the exercise of the power to register a code under the Act, prescribes that impact assessments should be conducted for 'all high privacy risk projects' in aid of good management and trust-building.[12] Rights seem to hardly feature in legal discourses around the impact assessments under the Act—including the Office of the Australian Information Commissioner's published guidance on the conduct of privacy impact assessments, which characterises these assessments as 'reasonable steps to implement practices, procedures and systems that will ensure compliance with the [Act's Australian Privacy Principles] APPs and enable them to deal with enquiries or complaints about privacy compliance', thus forming part of the 'risk management and planning processes' that entities should undertake.[13]

On the other hand, it is also clear that the publics in Australia, as in Europe, value privacy highly even when weighed against other rights and freedoms such as security and freedom of expression and indeed want to find ways to provide for all of these at the same time. For instance, an Oxford Internet Institute-INSEAD survey conducted in 2011 shows that Australian and European countries are relatively close in terms of their citizens' preferences to have 'it all' when it comes to these rights and freedoms.[14] Indeed, the authors find 'a global culture developing around the Internet, in which users worldwide share similar values and attitudes related to online freedom of expression, privacy, trust, and security'.[15] These concerns, especially centred on the processing of personal data, have only increased in recent years. For instance, the Office of the Australian Information Commissioner's (OAIC) Australian Community Attitudes to Privacy Survey 2020 records that 'seventy percent [of those surveyed] consider the protection of their personal information to be a major concern in their life'.[16] And a 2019 Eurobarometer survey finds that (even with the GDPR's protections) 'more than six out of ten are concerned about not having complete control over the information they provide online'.[17]

The Dutch and Australian governments' awareness of such public concerns no doubt lay behind their readiness to conduct very public impact assessments when it came to the introduction of their contact-tracing apps, which, by their nature, required a high degree of public trust to succeed as networked technologies (meaning that their value depended on how many people downloaded and used the app).[18] As we will see, the Dutch assessments of its CoronaMelder app were more squarely focused on rights. But, even in Australia, the government was eager to assuage public fears about the privacy impacts of its COVIDSafe app and appreciated that its public messaging around its impact assessment could not be restricted to narrow compliance with prevailing legal standards but should also take into account public concerns about rights and freedoms. Even so, query if its impact assessment went far enough in assuaging these concerns, as shown by the low trust ultimately placed in the app by prospective Australian users. That the Dutch app did better is a testament to its more rigorous rights-oriented impact assessments (although we might still query whether it did well enough compared to manual contact tracing to justify its deployment and use or whether the resources might have been better expended in other ways).

Related to the above was the lack of public participation and engagement provided for in the Australian impact assessment, certainly in comparison to the Dutch impact assessments. As Yeung and Bygrave explain, if the task of a privacy or data protection impact assessment is not just one of ensuring compliance with standards but maintaining public 'legitimacy',[19] then 'community-based governance' plays a distinct role here.[20] In our discussion below, we suggest that the effort made by the

[12] OAIC, 2017, Privacy, cls 12 and 4 (preamble).
[13] See OAIC, 2021b.
[14] Dutta, "The New Internet World," 3.
[15] Dutta, "The New Internet World," 3.
[16] OAIC, COVIDSafe Report, 4.
[17] Special Eurobarometer 487a, The General Data, 14.
[18] Leins, "Tracking, Tracing, Trust"; Burdon, "Implementing COVIDSafe." See generally van Slyke, "Perceived Critical Mass."
[19] Yeung, "Demystifying the Modernized," 138; cf. Metcalf, "Algorithmic Impact Assessments and Accountability"; Selbst, "An Institutional View."
[20] Yeung, "Demystifying the Modernized," 142.

Dutch Government to provide for wide consultation in its impact assessments paid off in terms of a better-designed app that was more broadly conversant with human rights (in other words, they represented a step in the right direction), and was also more trusted—and this should now be taken further in framing a future impact assessment process for pandemic times to recognise and incorporate a right of social dialogue as an essential feature of the process.

2.1. The COVIDSafe 'Experiment in Coercion'

Australia rolled out its COVID Bluetooth contact-tracing apps a few months into the pandemic as part of its effort to 're-open Australian society after the national and state lockdowns occasioned by the "first wave" of infections from March to May 2020'.[21] As with other contact-tracing apps, the intention was to have a digital contact-tracing app that complemented manual contact tracing in the shortest time, involving as many people as possible. What may be less obvious, given the high level of public take-up needed for the apps to succeed, was that it was not mandated or strongly pushed as, for instance, in Singapore.[22] Rather, the government relied on voluntary take-up of the apps, which, in turn, required a focus on public trust.[23] That this would be a particular challenge in Australia was partly because, as part of its 'distinctive experimental path to combatting the pandemic, which involves considerable amounts of coercion',[24] the government determined early on that it would adopt a centralised reporting architecture, here taking the Singapore TraceTogether app as its model. As foreshadowed above, the 'solution' found to the challenge of ensuring sufficient public engagement and trust for the app to succeed was to undertake and publicly vaunt a privacy impact assessment.[25] But this did little to forestall and may even have helped to engender the 'furious debate' surrounding the app.[26]

The privacy impact assessment, broadly speaking, followed the style of an impact assessment process set down in § 33D of the Privacy Act 1988, further elaborated in the OAIC Code and Guidance (noted earlier).[27] However, it followed its own sui generis character and rather than being directed by the Privacy Commissioner, it was directed by the government agency involved, namely the Department of Health. The impact assessment prepared by the law firm Maddocks made 18 recommendations highlighting issues of legal and technical compliance, which the government implemented.[28] Even so, the app had a relatively low uptake of 6.3 million downloads over the first few months,[29] that is, less than 25% of the population and well below the government's stated goal of 40%.[30] In part, this could be attributed to technical problems with its usability (the app required a smartphone with an Australian SIM card, was widely considered not easy to use and had a tendency to provide 'bad app' data, especially at the start).[31] There were also factors to do with low rates of COVID-19 infection in Australia in 2020, border closure policies and alternative options of QR code check-ins in states and territories from around the end of 2020, beginning in New South Wales (September) and Victoria (November). But, as Paul Garrett and Simon Dennis point out, there were broader problems with the app, noting that '[a] "social license" is necessary for any voluntary measure to be effective, and right now COVIDSafe doesn't have it'.[32]

Public perceptions of issues inter alia about the app's ability to offer effective protection of privacy and security indeed presented significant challenges in rolling out the app (potentially impacting both download and use rates). As reported in *The Lancet*, concerns about the app's reliance on a centralised database were 'identified early by many commentators as potential barriers for acceptance of the COVIDSafe app'.[33] Further, community experts openly complained that, although the app's source code was shared in May 2020 via GitHub, it was not properly open-sourced, and feedback was blocked—this, of course, did not prevent them from publishing their own concerns relating to the app's protection of privacy and security (based on what was publicly available).[34] Legal scholars also raised concerns about the available protection of privacy under the current terms of the Act and argued for law reform to increase transparency and accountability obligations.[35] The government, in its publicity, insisted that the app met high standards in both privacy and security. And in an effort to strengthen public confidence along

[21] Goggin, "COVID-19 Apps," 63. See also Greenleaf, "Australia's 'COVIDSafe' Law."
[22] Goggin, "COVID-19 Apps," 63.
[23] Greenleaf, "Australia's 'COVIDSafe' Law," 259.
[24] Greenleaf, "Australia's 'COVIDSafe' Law," 260.
[25] Burdon, "Implementing COVIDSafe".
[26] Goggin, "COVID-19 Apps," 63.
[27] See OAIC, 2017; OAIC, 2021b.
[28] Department of Health, COVIDSafe Application Privacy Impact Assessment.
[29] Hunt, "The COVIDSafe App."
[30] Leins, "Tracking, Tracing, Trust," 6.
[31] See Silver, "Smartphone Ownership"; Nelson, Report on the Operation; Greenleaf, "Australia's 'COVIDSafe' Law."
[32] Garrett, "Australia Has All But Abandoned."
[33] Vogt, "Effectiveness Evaluation," 255.
[34] Nelson, Report on the Operation, 4.
[35] See especially Greenleaf, "Australia's 'COVIDSafe' Law"; Burdon, "Implementing COVIDSafe."

with expert involvement, amendments to the Privacy Act were introduced to provide an explicit oversight role for the OAIC, limit the app's personal data collection, use and disclosure to the specific purposes of contact tracing and state that data collected must be held in Australia and deleted when the app was no longer in use.[36] The OAIC also conducted its own review of various aspects of COVIDSafe, finding only a handful of medium and low-risk deficiencies that it suggested could be relatively easily addressed.[37] Even so, the public's distrust in the app's protection of privacy and security persisted over the life of the app, along with rising 'fear[s] of the normalisation of governmental tracking',[38] as well as digital exclusion with different levels of access and affordability detected for Australians with low incomes, education and employment levels (the 65 years and older group), Indigenous Australians, those with disabilities and Australians living in remote and regional areas.[39]

In the final wrap-up, according to Department of Health data, only two positive COVID-19 cases were identified through the app, which were not found by manual contact tracers.[40] And, despite 7.9 million registrations of the COVIDSafe app between April 2020 and May 2022, only 792 consented to their data being added to the centralised data store for contact tracing.[41] The Department of Health did not reflect on the reasons for the app's failure while reporting on it.[42] But, following a change of government, the new Health Minister Mark Butler, on announcing the app's decommission in August 2022, scathingly denounced the 'wasteful and ineffective COVIDSafe app' as a 'colossal waste of more than $21 million of taxpayers money'.[43]

2.2 The CoronaMelder Exemplar of 'Technology Theatre'

By contrast with the failed Australian COVIDSafe app along with its rather limited impact assessment, the Dutch CoronaMelder app, supported and tested by its impact assessments, presents an exemplar of technical competence and human rights compliance. Yet, as Rosamunde van Brakel et al. point out, there was a certain amount of 'technology theatre' going on here, which may help to explain the app's ultimately limited success in tackling a pandemic that required a massive human effort in trust and cooperation.[44] Despite all the laudable efforts in creating and deploying a well-designed contact-tracing app that the public would readily accept and use, and with a reasonable level of public participation, with some 4.6 million users downloading the app (i.e., about 30% of the country's population),[45] the app enhanced the effectiveness of manual contact tracing by a mere 6%.[46] Even those taking a positive view describe its effects as 'small'.[47] Meanwhile, according to ex post efficiency assessments, manual contact tracing was still a significantly preferable alternative in terms of its effectiveness in detecting infections.[48] This leaves the question of what type of impact assessment would achieve a better outcome in terms of effectiveness without unduly derogating from rights or whether the project should have been abandoned to start with.

As a technology, CoronaMelder seems hard to fault. It combined a decentralised client-server Bluetooth architecture with decentralised privacy-preserving proximity (DP-3T) protocols that worked on iOS and Android smartphones. From inception to rollout and use, its development was an open and transparent open-source collaborative work-in-progress process, with all intermediate app versions shared in GitHub. Its design was fully aligned with the GDPR—meeting the required robustness and data protection requirements such as data minimisation, data protection by default and design and storage restrictions. Moreover, it was fully tested throughout the app's design, development and rollout. The large-scale field testing involved 2,000 users during the mid-design, and this was followed by final practice testing in different regions two weeks before rollout. And consideration was given to users with restrictions such as age (60+ group) and visual, minor mental or motor impairments, with usability testing aimed to make the app user-friendly for these users.[49]

Likewise, the various impact assessments were also generally well-designed and conducted. Two official data protection impact assessments were conducted pursuant to art. 35 of the GDPR, with both made publicly available. The first, from July 2020, was conducted under the auspices of the Ministry of Health, Welfare and Sports. This revealed no major risks associated with the

[36] *Privacy Amendment (Public Health Contact Information) Act 2020* (Cth).
[37] OAIC, 2021a. See also OAIC, COVIDSafe Report; Blight, Report to OAIC.
[38] Vogt, "Effectiveness Evaluation," 255.
[39] Smoll, "The Barriers." See also Thomas, "Concerns"; Social Research Centre, "Increasing COVIDSafe App Usage."
[40] Department of Health, Third Report.
[41] Department of Health, Third Report.
[42] Department of Health, Third Report.
[43] Butler, "Failed."
[44] van Brakel, "Bridging Values," 56. See also McDonald, "Technology Theatre."
[45] van Brakel, "Bridging Values," 53 citing van der Laan et al. (2021).
[46] Boncz, "An Epidemiological Model," 12.
[47] Boncz, "An Epidemiological Model," 12.
[48] Boncz, "An Epidemiological Model," 12. Cf. Poort, "CoronaMelder."
[49] van Brakel, "Bridging Values," 52.

app's operation, and the app was judged as a necessary and proportionate measure in the circumstances.[50] The second, from August 2020, was conducted by the law firm Privacy Management Partners (a firm with extensive expertise in data protection),[51] and this found that the app was largely sufficient in addressing the data protection standards. Nor were the assessments confined to technical and legal compliance. Ethical and social implications also received attention in the above reviews. And in a further review of the app, a range of core ethical values compiled by a panel of professionals and citizens coordinated by technology ethicist Peter-Paul Verbeek were emphasised as key to 'social embedding of the app', with 'inclusiveness' and 'solidarity' highlighted as among the important values here.[52] As can be seen from the above discussion, expertise and diverse participation were features of these assessments, with the teams involved including officials, scientists and technologists, legal experts, behavioural science expertise on how the app could support control and follow-up of infections, ethical experts such as Verbeek (as noted above), along with diverse other individuals and community representatives who participated in the app's testing phases to help improve its functionality, effectiveness and acceptability in ethical and social terms.

Nevertheless, despite the extraordinary level and breadth of the impact assessments conducted on the CoronaMelder app, there were some omissions. In particular, the second impact assessment conducted by Privacy Management Partners noted some broader social issues although outside the scope of the terms of reference, such as the fact that those at the frontline—such as healthcare workers, shop assistants and transport workers—may be disproportionately burdened by notifications and may ultimately turn off rather than embracing the app. Additionally, there were uncertain ramifications of introducing populating monitoring technologies in the longer term.[53] An independent study conducted by social researchers from the University of Twente and North-West University further found that the CoronaMelder app was generally easy to use, but some participants, particularly older adults, young people with more limited education or disability and adults of migrant background, found it more difficult to deal with. There were also various concerns expressed about the app's usefulness and privacy-preserving mechanisms, with the researchers suggesting the need for better and more targeted communication.[54] Might these challenges have been overcome with even wider and more inclusive consultation in the impact assessments conducted on the app, or might the app itself have come more into question with those consulted arguing for more emphasis on manual contact tracing and human support, possibly in combination with the app and/or other measures? At the very least, it can be concluded that even in the Dutch case, for all its advantages over the Australian one, '[c]areful assessments of technological solutions in crisis situations are needed', involving a full range of participants.[55]

3. Framing a Data Rights Impact Assessment Process

The above case studies reinforce the point made by Yeung and Bygrave that paying attention to ethics and social norms, including around human rights and establishing community-based governance, need to be central features of an impact assessment process geared to establishing and maintaining public 'legitimacy'.[56] In the words of the EU's European Group on Ethics in Science and New Technologies, 'human beings ought to be able to determine which values are served by technology, what is morally relevant and which final goals and conceptions of the good are worthy to be pursued'.[57] There are also more practical reasons for taking this line. As Charles Raab explains, at their best, impact assessments serve as 'mechanisms for learning, not only because of the information they bring to light and disseminate about the functioning of technologies and systems, but because of the way such information might generate better handles on what works or what is more likely to work better'.[58] Or, as Alessandro Mantelero puts it, 'participation can give voice to the different groups of persons potentially affected by the use of data-intensive systems and different stakeholders (eg NGOs, public bodies) facilitating a human-centred approach to AI design'; while, at the same time, it 'reduces the risk of under-representing certain groups and may also flag up critical issues that have been underestimated or ignored'.[59] For instance, as noted above, it may be hoped that (even) wider and more inclusive public consultation would have 'flagged up' concerns around inter alia privacy and other data rights implications of the Australian and Dutch contact-tracing apps as well as assisting with the development of effective responses—including deciding whether the app was worthwhile (in its current state) and if so on what terms, whether communication around the app

[50] Ministerie van Volksgezondheid, Gegevensbeschermingseffectbeoordeling, 28; 31; 38ff (Bijlage 1: Risico's en Maatregelen).
[51] Privacy Management Partners, Second Opinion.
[52] Verbeek, Ethische Analyse, 6.
[53] Privacy Management Partners, Second Opinion, 6.
[54] Bente, "The Dutch," 1, 15–16.
[55] van Brakel, "Bridging Values," 56; Verbeek, Ethische Analyse, 8.
[56] Yeung, "Demystifying the Modernized," 138, 142.
[57] European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, 9–10. Cf. Yeung, A Study of the Implications, 8, 35–36.
[58] Raab, "Information Privacy," 14.
[59] Mantelero, Beyond Data, 18.

might be better delivered to diverse communities or whether resources should be allocated in some other way. More overt attention paid to accommodating public concerns, including with respect to rights, may also have improved the prospects of public trust in these technologies that relied on public trust to succeed. But ultimately, we think the value of these inclusive initiatives should not depend solely on such immediate practical considerations. If 'legitimacy' means 'social licence',[60] that is, public acceptability in a society that is grounded in democracy, then paying attention to what relevant publics consider important is of value. Likewise, it can reasonably be argued that a 'truly trustworthy' technology is one in which 'trust is based on respect for human rights, democracy and the rule of law'.[61] And if 'rights' are grounded in notions of human dignity and liberty, these should be understood to include 'the right to be free to set one's own standards and choose one's own goals'[62] and 'to participate in decision-making in matters which affect [one's] rights'[63]—including with respect to data, and in balance with other rights, freedoms and interests applying a proportionality analysis.[64]

In short, what we are arguing for is a right to social dialogue in relation to the deployment and use of novel pandemic technologies that affect the rights of humans with respect to their data. This is a right that can be viewed as implicit in the rights-centric principles of a modern privacy/data protection regime, like the EU GDPR, which (as Yeung and Bygrave argue) should be broadly construed as a progressive instrument in line with its character and goals,[65] and like the Australian Privacy Act, which although less modern than the GDPR specifies the right to privacy in the United Nations' International Covenant on Civil and Political Rights (to which Australia is a party) as a guiding principle along with the rest of that covenant, which includes provisions on freedom of expression, freedom of association, and self-determination for 'all peoples'.[66] It is a right that we have in previous writing identified as important in relation to algorithmic decision-making technologies where the points of view of data subjects (as voiced by them or their chosen representatives, or both) need to be taken into account.[67] But it also makes sense in relation to the deployment and use of a wider range of pandemic technologies that impact data rights, given their applications across large sections of the community, their implications for human welfare, their potential health and life-giving aspects and the emergency conditions under which decisions are made and applied—including a temptation for governments to turn to 'new technologies as a policy response to crisis'.[68] We see it as part and parcel of a general approach to pandemic decision-making that reflects values such as 'preparedness and management',[69] transparency and trustworthiness,[70] inclusiveness and solidarity[71] and respect for human rights.[72] We would hope (and expect) it would lead to better decision-making accommodating diverse individuals and communities, at the same time enhancing their trust in 'truly trustworthy' technologies. The right to engage in social dialogue on the deployment and use of pandemic technologies that impact humans and their data is a matter of human dignity and liberty and respect for rights, including rights around data. But its basic value lies in the recognition that this right should be not only an end goal but a part of the process leading up to that end, including—indeed especially—in pandemic times.

4. Conclusion

In this article, we have argued that an impact assessment process for pandemic technologies that impact data rights should provide for a right of social dialogue as part of the process. With Australia coming to recognise the value of impact assessments in addressing prospective social harms associated with novel technologies,[73] the question is whether policymakers of the future will learn from the salutary experience of the (rather limited) impact assessment commissioned and conducted with respect to the COVIDSafe contact-tracing app as detailed in our first case study, which failed to address and assuage public concerns about the treatment of sensitive personal data, the prospect of unwanted surveillance and the discriminatory effects for marginalised individuals and communities. And we suggested that there is much to be learned from the more broadly expert and consultative Dutch impact assessments for the Corona Melder app considered in our second case study, even if we also

[60] Garrett, "Australia Has All But Abandoned." See also Yeung, "Demystifying the Modernized," 138; and *passim*.
[61] Mantelero, Beyond Data, 82. Cf. Burdon, "Implementing COVIDSafe." See generally O'Neill, "Linking Trust."
[62] European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, 9. Cf. Yeung, A Study of the Implications, 35–36; Committee on Artificial Intelligence, "Towards an Application."
[63] See (specifically re: Indigenous Peoples) UN Declaration on the Rights of Indigenous Peoples (UNDRIP), art. 18; Lovett, "Good Data Practices," 30; and *passim*. Cf. (in Australia) Dudgeon, "Mental Health"; Morrissey, "An Australian," 91.
[64] See Group of Chief Scientific Advisors to the European Commission, Improving Pandemic Preparedness, 10.
[65] Cf. Yeung, "Demystifying the Modernized," 151–152.
[66] See ICCPR, arts 1, 19, and 22. See also UNDRIP, arts 18 and 19. See generally Lovett, "Good Data Practices."
[67] See GDPR, art 22; Clifford, "A Right," 1–9. Cf. Lazcoz, "Humans."
[68] McDonald, "Technology Theatre."
[69] See Group of Chief Scientific Advisors to the European Commission, Improving Pandemic Preparedness, 9.
[70] See Palmiotto, "Tracing Transparency." See also Mantelero, Beyond Data, 18.
[71] Recalling Verbeek, Ethische Analyse, 8. See also Mantelero, Beyond Data, 191.
[72] Cf. Mantelero, Beyond Data, 191.
[73] Attorney-General's Department, Privacy Act Review, proposal 13.1.

suggested there was scope for improvement there as well—with some further guidance sketched out in the appendix below. Hopefully, next time around, a wide range of expertise and experience of diverse individuals and communities will be drawn on in the impact assessments for technologies designed to alleviate a pandemic's threats of harm to life and health but at what cost to privacy and other data rights?

Appendix: Guidance for a Data Rights Impact Assessment Process for Pandemic Technologies

Key elements	(A) Official input, expertise	(B) Social dialogue
1. Technical proficiency	Ensure expert timely assessment of technical aspects of the technology throughout its lifecycle, including with respect to data minimisation, security and safety, transparency and consent, encryption, coding and tracking schemes and the storage of data.	Encourage and facilitate wide public consultation with diverse individuals and groups who will be affected by the technology, as well as community experts and representatives and civil society activists, with a particular emphasis on the technical features of the technology.
2. Legal requirements (including with respect to rights)	Ensure expert assessment of compliance with legal requirements in relation to the deployment and continued use of the technology, including with respect to privacy data and other human rights standards broadly construed.	Encourage and facilitate wide public consultation with diverse individuals and groups who will be affected by the technology, as well as community experts, representatives and civil society activists, with a particular emphasis on legal standards that, broadly construed, protect rights, freedoms and interests.
3. Broader ethical and social standards (including with respect to rights)	Ensure expert assessment of the extent to which the technology meets ethical standards and social norms, including with respect to privacy, data and other human rights aspects broadly construed.	Encourage and facilitate wide public consultation with diverse individuals and groups who will be affected by the technology, as well as community experts, representatives and civil society activists, with a particular emphasis on ethical standards and social norms that speak to rights, freedoms and interests.

Acknowledgements
The authors are grateful to Karin Clark, Kobi Leins, Vanessa Teague, Martin Vranken and the editor and reviewers for *Law, Technology and Humans* for their very helpful comments and insights.

Bibliography

Article 29 Working Party. *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679*. European Commission, 2017. https://ec.europa.eu/newsroom/article29/items/611236.

Attorney-General's Department, Australian Government. *Privacy Act Review—Report 2022*. https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

Bente, Britt Elise, Jan W. J. R. van't Klooster, Maud A. Schreijer, Lea Berkemeier, Joris E. van Gend, Peter J. H. Slijkhuis, Saskia M. Kelders and Julia E. W. C. van Gemert-Pijnen. "The Dutch COVID-19 Contact Tracing App (the CoronaMelder): Usability Study." *JMIR Formative Research* 5, no 3 (2021): e27882. https://doi.org/10.2196/27882.

Blight, Jake. *Report to OAIC on COVID App Data, 16 May to 16 November 2020*. Inspector-General of Intelligence and Security, 2020. https://www.documentcloud.org/documents/20416358-report-to-oaic-may-nov-2020-covidsafe-app#document/p2/a2005851.

Boncz, Peter. "An Epidemiological Model for Contact Tracing with the Dutch CoronaMelder App." *arXiv preprint arXiv:2105.15111 v3* (2021). https://doi.org/10.48550/arXiv.2105.15111.

Burdon, Mark and Brydon Wang. "Implementing COVIDSafe: The Role of Trustworthiness and Information Privacy Law." *Law, Technology and Humans* 3, no 1 (2021): 35–50. https://doi.org/10.5204/lthj.1808.

Butler, Mark (Hon). "Failed COVIDSafe App Deleted." Media release, August 10, 2022. On the Department of Health and Aged Care website. https://www.health.gov.au/ministers/the-hon-mark-butler-mp/media/failed-covidsafe-app-deleted#:~:text=The%20Hon%20Mark%20Butler%20MP&text=10%20August%202022-,The%20Albanese%20Government%20has%20acted%20to%20delete%20the%20wasteful%20and,money%20on%20this%20failed%20app.

Committee on Artificial Intelligence. "Towards an Application of AI Based on Human Rights, the Rule of Law and Democracy." Council of Europe. 2023. https://coe.int/en/web/artificial-intelligence/cai.

Clifford, Damian, Jake Goldenfein, Aitor Jiminez and Megan Richardson. "A Right of Social Dialogue on Automated Decision-Making: From Workers' Right to Autonomous Right." *Technology and Regulation* 2023 (2023): 1–9. https://doi.org/10.26116/techreg.2023.001.

Council of Europe. *European Convention for the Protection of Human Rights and Fundamental Freedoms*. France: European Court of Human Rights, November 4, 1950. https://www.echr.coe.int/documents/convention_eng.pdf.

Department of Health. *COVIDSafe Application Privacy Impact Assessment (Agency Response, 2020).*

Department of Health. *Third Report on the Operation and Effectiveness of COVIDSafe and the National COVIDSafe Data Store*. Department of Health and Aged Care, last updated August 11, 2022. https://www.health.gov.au/resources/publications/third-report-on-the-operation-and-effectiveness-of-covidsafe-and-the-national-covidsafe-data-store.

Dudgeon, Pat, Joanna Alexi, Kate Derry, Tom Brideson, Tom Calma, Leilani Darwin, Paul Gray, Tanja Hirvonen, Rob McPhee, Helen Milroy, Jill Milroy, Donna Murray and Stewart Sutherland. "Mental Health and Well-Being of Aboriginal and Torres Strait Islander Peoples in Australia during COVID-19." *Australian Journal of Social Issues* 56, no 4 (2021): 485–502. https://doi.org/10.1002/ajs4.185.

Dutta, Soumitra, William H. Dutton and Ginette Law. "The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online." *INSEAD Working Paper No 2011/89/TOM* (2011). http://dx.doi.org/10.2139/ssrn.1916005.

European Group on Ethics in Science and New Technologies. *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*. Brussels: European Commission, Directorate-General for Research and Innovation, 2018. https://op.europa.eu/en/publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1.

European Union (EU). "Charter of Fundamental Rights of the European Union 2012/C 326/02." *Official Journal of the European Union* 326 (October 26, 2012): 391–407 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:C2012/326/02.

European Union. "Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)." *Official Journal of the European Union* 119 (2016): 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Garrett, Paul M. and Simon J. Dennis. "Australia Has All But Abandoned the COVIDSafe App In Favour of QR Codes (So Make Sure You Check In)." *The Conversation*, June 1, 2021. https://theconversation.com/australia-has-all-but-abandoned-the-covidsafe-app-in-favour-of-qr-codes-so-make-sure-you-check-in-161880.

Goggin, Gerard. "COVID-19 Apps in Singapore and Australia: Reimagining Healthy Nations with Digital Technology." *Media International Australia* 177, no 1 (November 2020): 61–75. https://doi.org/10.1177/1329878X20949770 .

Greenleaf, Graham and Katherine Kemp. "Australia's 'COVIDSafe' Law for Contact Tracing: An Experiment in Surveillance and Trust." *International Data Privacy Law*, no 11 (2021): 257–275. https://doi.org/10.1093/idpl/ipab009.

Group of Chief Scientific Advisors to the European Commission, European Group on Ethics in Science and New Technologies and Special advisor to President Ursula von der Leyen on the response to the coronavirus and COVID-19—Professor Peter Piot. *Improving Pandemic Preparedness and Management*. Brussels: European Commission, November 11, 2020. https://op.europa.eu/o/opportal-service/download-handler?identifier=a1016d77-2562-11eb-9d7e-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=.

Hunt, Greg (@TheHonGregHunt). 2020. "The COVIDSafe App continues to protect our families, communities & frontline health workers." Twitter, June 19, 2020, 2:10 a.m. https://twitter.com/greghuntmp/status/1273724682404007938?lang=en.

Kaminski, Margot E. "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability." *Southern California Law Review* 92 (2019): 1529–1616. https://dx.doi.org/10.2139/ssrn.3351404.

Kaminski, Margot E. and Gianclaudio Malgieri. "Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations." *International Data Privacy Law* 11, no 2 (2021): 125–144. https://doi.org/10.1093/idpl/ipaa020.

Kasirzadeh, Atoosa and Damian Clifford. "Fairness and Data Protection Impact Assessments." *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (2021): 146–153. https://doi.org/10.1145/3461702.3462528.

Kosta, Eleni. "Article 35 Data Protection Impact Assessment." In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A Bygrave, Christopher Docksey and Laura Drechsler, 665–679. Oxford: Oxford University Press, 2020. https://doi.org/10.1093/oso/9780198826491.003.0072.

Lazcoz, Guillermo and Paul de Hert. "Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems. Essential Pre-Requisites Against Abdicating Responsibilities." *Computer Law & Security Review* 50 (2023): 1–20. https://doi.org/10.1016/j.clsr.2023.105833.

Leins, Kobi, Christopher Culnane and Benjamin I. P. Rubinstein. "Tracking, Tracing, Trust: Contemplating Mitigating the Impact of COVID-19 Through Technological Interventions." *The Medical Journal of Australia* 213, no 1 (2020): 6–8. https://doi.org/10.5694/mja2.50669.

Lonergan Research. *Australian Community Attitudes to Privacy Survey 2020*. Office of the Australian Information Commissioner, 2020. https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf.

Lovett, Raymond, Vanessa Lee, Tahu Kukutai, Donna Cormack, Stephanie Rainie and Jennifer Walker. "Good Data Practices for Indigenous Data Sovereignty and Governance." In *Good Data*, edited by Angela Daly, S. Kate Devitt and Monique Mann, 26–36. Amsterdam: Institute of Network Cultures, 2019. https://hdl.handle.net/10289/12919.

Maddocks/Department of Health. *THE COVIDSAFE APPLICATION Privacy Impact Assessment (2020)*.

Mantelero, Alessandro. *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*. The Hague, Netherlands: TMC Asser Press, 2022. https://link.springer.com/book/10.1007/978-94-6265-531-7.

McDonald, Sean Martin. "Technology Theatre." *Centre for International Governance Innovation*, July 13, 2020. https://www.cigionline.org/articles/technology-theatre.

Metcalf, Jacob, Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh and Madeleine Clare Elish. "Algorithmic Impact Assessments and Accountability: The Co-Construction of Impacts." *ACM Conference on Fairness, Accountability, and Transparency (FAccT 21)* (March 3–10, 2021). https://doi.org/10.1145/3442188.3445935.

Ministerie van Volksgezondheid, Welzijn en Sport. *Gegevensbeschermingseffectbeoordeling (DPIA) COVID-19 Notificatie-app*. July 7, 2020. https://www.rijksoverheid.nl/documenten/rapporten/2020/07/07/gegevensbeschermingseffectbeoordeling-dpia-covid-19-notificatie-app.

Morrissey, Philip. "An Australian First Nations COVID-19 Prevention Strategy and the Limits of a Medicalised Managerial Discourse." In *Indigenous Health and Well-Being in the COVID-19 Pandemic*, edited by Nicholas D. Spence and Fatih Sekercioglu, 81–93. Routledge, 2023. https://doi.org/10.4324/9781003220381-5.

Nelson, Richard, Vanessa Teague, Jim Mussared and Geoffrey Huntley. *Report on the Operation and Effectiveness of the COVIDSafe Application 26 April 2020 to 31 July 2021*. August 5th, 2021. https://t.co/LZpSaPgNGE?amp=1.

Organisation for Economic Co-operation and Development (OECD). *Building Trust to Reinforce Democracy: Key Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions*. Paris: OECD Publishing, 2021. https://doi.org/10.1787/b407f99c-en.

Office of the Australian Information Commissioner. *Privacy (Australian Government Agencies—Governance) APP Code*. 2017. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/australian-government-agencies-privacy-code/privacy-australian-government-agencies-governance-app-code-2017.

Office of the Australian Information Commissioner. *COVIDSafe Report May–November*. 2020. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/covid-19/covidsafe-reports/covidsafe-report-maynovember-2020.

Office of the Australian Information Commissioner. *COVIDSafe Assessment 3*: COVIDSafe Application Functionality, Privacy Policy and Collection Notices. 2021a. https://www.oaic.gov.au/privacy/privacy-assessments-and-

decisions/privacy-assessments/covidsafe-assessment-3-covidsafe-application-functionality,-privacy-policy-and-collection-notices.
Office of the Australian Information Commissioner. *Guide to Undertaking Privacy Impact Assessments*. 2021b. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments.
O'Neill, Onora. "Linking Trust to Trustworthiness." *International Journal of Philosophical Studies* 26, (2018): 293–300. https://doi.org/10.1080/09672559.2018.1454637.
Palmiotto, Francesca. "Tracing Transparency: Public Governance of Algorithms and the Experience of Contact Tracing Apps." In *Sovereignty, Technology and Governance after COVID-19: Legal Challenges in a Post-Pandemic Europe*, edited by Francisco de Abreu Duarte and Francesca Palmiotto, 77–102. Hart Publishing, 2022. https://cadmus.eui.eu/handle/1814/75178.
Poort, Joost. "CoronaMelder: An Economic Perspective." In *Conditions for Technological Solutions in a COVID-19 Exit Strategy, with Particular Focus on the Legal and Societal Condition*, 121–130. Institute for Information Law, 2021. https://ssrn.com/abstract=3945689.
Privacy Management Partners (mr drs Jeroen Terstegge CIPP/E, partner). *Second Opinion DPIA Corona Melder App*. August 19, 2020. https://zoek.officielebekendmakingen.nl/blg-944749.pdf.
Raab, Charles D. "Information Privacy, Impact Assessment, and the Place of Ethics." *Computer Law & Security Review* 37 (2020): 1–16. https://doi.org/10.1016/j.clsr.2020.105404.
Selbst, Andrew D. "An Institutional View of Algorithmic Impact Assessments." *Harvard Journal of Law & Technology* 35 (2021): 117–191. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3867634.
Smoll, Nicolas R., Jacina Walker and Gulam Khandaker. "The Barriers and Enablers to Downloading the COVIDSafe App—a Topic Modelling Analysis." *Australian and New Zealand Journal of Public Health* 45, no 4, (2021): 344–347. https://doi.org/10.1111/1753-6405.13119.
Social Research Centre. "Increasing COVIDSafe App Usage: Insights from an SRC Quick Poll." *Social Research Centre*, May 11, 2020. https://www.srcentre.com.au/our-research/life-in-australia-reports/covidsafe-update.
Special Eurobarometer 487a. *The General Data Protection Regulation*. European Commission, June 2019. https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf.
Silver, Laura. "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally." *Pew Research Center*. February 5, 2019. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/.
Thomas, Rae, Zoe A. Michaleff, Hannah Greenwood, Eman Abukmail and Paul Glasziou. "Concerns and Misconceptions about the Australian Government's COVIDSafe App: Cross-Sectional Survey Study." *JMIR Public Health Surveillance* 6, no 4 (2020). https://doi.org/10.2196/23081.
United Nations General Assembly. "International Covenant on Civil and Political Rights." *United Nations Treaty Series* 999 (December 16, 1966): 171. https://treaties.un.org/pages/showdetails.aspx?objid=0800000280004bf5.
United Nations General Assembly. *The United Nations Declaration on the Rights of Indigenous Peoples*. Department of Economic and Social Affairs, 2007. https://social.desa.un.org/issues/indigenous-peoples/united-nations-declaration-on-the-rights-of-indigenous-peoples.
van Brakel, Rosamunde, Olya Kudina, Chiara Fonio and Kees Boersma. "Bridging Values: Finding a Balance Between Privacy and Control. The Case of Corona Apps in Belgium and the Netherlands." *Journal of Contingencies and Crisis Management* 30, no 1 (2022): 50–58. https://doi.org/10.1111/1468-5973.12395.
van Slyke, Craig, Virginia Ilie, Hao Lou and Thomas Stafford. "Perceived Critical Mass and the Adoption of a Communication Technology." *European Journal of Information Systems* 16, no 3 (2007): 270–283. https://doi.org/10.1057/palgrave.ejis.3000680.
Verbeek, Peter-Paul *Ethische Analyse van de COVID-19 Notificatie-App ter Aanvulling op Bron en Contactonderzoek GGD Deel 2: Analyse Door Burgers en Professionals*. September 10, 2020. https://ecp.nl/wp-content/uploads/2020/11/rapport-begeleidingsethiek-coronamelder.pdf.
Vogt, Florian, Bridget Haire, Linda Selvey, Anthea L. Katelaris and John Kaldor. "Effectiveness Evaluation of Digital Contact Tracing for COVID-19 in New South Wales, Australia." *The Lancet* 7, no 3 (2022): E250–E258. https://doi.org/10.1016/s2468-2667(22)00010-x.
Yeung, Karen. *A Study of the Implications of Advanced Digital Technologies (including AI systems) for the Concept of Responsibility within a Human Rights Framework*. Council of Europe, September 5, 2019. https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdab.
Yeung, Karen and Lee A. Bygrave. "Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship." *Regulation & Governance* 16 (2022): 137–155. https://doi.org/10.1111/rego.12401.

Primary Legal Material

Privacy Amendment (Public Health Contact Information) Act 2020 (Cth)