Article

Alternative Law Journal
2020, Vol. 45(3) 162–167

DOI: 10.1177/1037969X20930431
journals.sagepub.com/home/altlj
SAGE

The COVID cyborg: Protecting data status

Kate Galloway
Griffith Law School, Griffith University, Australia

Abstract
This article examines the increasing tendency towards governance of people through their representation via data. In its most contemporary iteration, the COVID-19 pandemic has seen the release of contact tracing apps – in Australia, COVIDSafe. While public discourse about the apps has focused principally on the important issue of data privacy, there are other possible effects whereby participation in such schemes might become a prerequisite to accessing services or basic rights – either from government or from corporations. The pathway to acceptability of applying our data in this way is already paved, through fitness monitors and other technologies by which we represent ourselves. This article sets out the foundation of such technologies and their application, before outlining their effect on the recognised boundaries of governance and the conception of the holder of rights and the substance of those rights.

Keywords
Data, democracy, discrimination, human rights, public health law & policy

In 2018, biohacker Meow-Ludo Disco Gamma Meow-Meow was found guilty of travelling on Sydney buses without a valid ticket.[1] Rather than carrying Sydney public transport's Opal card with him, he had instead implanted its chip into his hand. He had indeed tapped on when entering the bus – so had paid for his trip. However, Sydney transport authorities were not satisfied with this, alleging that he had breached the card's terms of use.

Meow-Meow claimed that his case was based on the principle of 'cyborg rights'.[2] The modification of his body through embedding technology-capable hardware is a feature of a posthuman evolution, a 'leaky distinction between animal-human and machine'.[3] As an activist pushing the boundaries of the definition of human, Meow-Meow was simultaneously pushing the boundaries of the rights held by an altered human before the law.

This article suggests that the COVID-19 pandemic will test the boundaries of our personhood in a new way. Despite the existing state/corporate data infrastructure whereby others are able to construct a picture of our most intimate lives,[4] there is not yet a universally compelling basis for production of personal data as a threshold for acceptance into places or institutions. Contact tracing may present one. If our data are to be carried with us as an integral and qualifying part of our interface with the world around us, it may be considered as part of our person. To the extent that our data

[1]The case is unreported but was widely reported in the media. See, eg, Lily Mayers 'Sydney Bio-Hacker Who Implanted Opal Card into Hand Fined for not Using Valid Ticket', *ABC News* (online, 16 March 2018) https://www.abc.net.au/news/2018-03-16/opal-card-implant-man-pleads-guilty-transport-offences/9555608.

[2]See, eg, Chris Hables Gray, *Cyborg Citizen: Politics in the Posthuman Age* (Routledge, 2000).

[3]Donna Haraway, 'A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century' in Haraway, *Simians, Cyborgs and Women: The Reinvention of Nature* (Routledge, 1991) 149, 152. The work was originally published as 'A Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980s' (1987) 2(4) *Australian Feminist Studies* 1.

[4]Kate Galloway, 'Big Data, Government, Privacy and Human Rights' in Paula Gerber and Melissa Castan (eds), *Contemporary Perspectives on Human Rights Law in Australia Volume 2* (Thomson Reuters, in press).

Corresponding author:
Associate Professor Kate Galloway, Griffith Law School, Griffith University, Kessels Road, Nathan, QLD 4111, Australia.
Email: kate.galloway@griffith.edu.au

engagement differentiates us from other humans, the question arises of the protections available at law. In particular, with an 'extended' human such as Meow-Meow, the question arises about where recognised boundaries of governance lie, whether the extended human is the bearer of rights, and if so, what is the substance of those rights.

The second part of this article outlines the basis on which our data are effectively an extension of ourselves, and as such constitutes the extended human as a species of 'cyborg' following Haraway's interpretation.[5] The third, and final, section analyses social contexts that may prefer, or demand, what I call here a 'COVID cyborg' – a person enhanced by their COVID tracing data[6] – to the exclusion of those not so enhanced. It envisages our society comprising two classes of people differentiated by their data status: the COVID cyborg and those who are app free. Unlike the experience of Meow-Meow, the COVID cyborg is likely to be embraced, effectively affording them rights superior to those who are app free. If this is to be the case, the law needs to comprehend both cyborg and the app free as equal subjects of protection.

Body + data: The cyborg self

While Meow-Meow's choice of body modification might appear extreme to some, the science fiction-like nature of human technological enhancement is occurring in more prosaic ways. A pacemaker, for example, might transmit data about its human operating system in the same way that Meow-Meow's Opal card chip transmitted data concerning payment of a bus fare.[7] Whether therapeutic interventions properly constitute a 'cyborg' remains an open question; however, to the extent that they might, the pacemaker example certainly poses less of a challenge to our general conceptions of humanity than does a more extreme bodily modification, possibly undertaken by oneself.[8]

Machines and other hardware (and software) may be implanted within us, but more readily we are enhancing our physical capabilities by carrying them on our person. Smartphones are ubiquitous, and as they extend our intellectual capacity, ability to communicate, and even provide biophysical feedback for lifegiving treatments,[9] so too do they track our locations and share myriad personal data with government and corporations alike. Fitness trackers worn on the wrist measure our physiological signs not only re-presenting them to their wearer as a variety of metrics by way of graphs and icons, but also sharing with other users and their corporate creators. Our devices also call for biometric data to unlock their features. We readily submit to fingerprints and facial recognition, granting global corporates the most intimate of insights into ourselves.

At the same time as we have willingly released aspects of ourselves, through our data, in the private sphere our government has constructed a surveillance architecture affording security services wide scope for access to our telecommunications data[10] and our biometric data[11] without our permission and often without our knowledge. Although governments have pushed through the suite of legislation for over a decade,[12] this has not come without a cost. The uptake of My Health Record, a putative personal database of one's medical information, has been poor.[13] And now, in the thrall of a pandemic, the Australian government has released a contact tracing app called COVIDSafe, whereby a user's proximity to another person (within 1.5 m for more than 15 minutes) would be identified through Bluetooth technology, encrypted, and recorded in the app. If a user is diagnosed with COVID-19, then the user would upload their data to the health department, and all contacts would be notified of the infection.

Critique of the app, released on 26 April 2020, has generally been concerned with data privacy per se. This is, of course, important. However, independently of data privacy is a question the opposite to that encountered by Meow-Meow. For the foreseeable future, and particularly while we are in a declared public health emergency,[14] our infection status regarding COVID-19 is central to our freedom, and indeed, to wider societal freedom. In that sense, a tracing app – and its data – effectively functions as an extension of ourselves. They are a means of reassurance not only to public health officials running the program, but to wider society, that we, collectively,

[5]Haraway (n 3).

[6]See Paul Farrell, 'Here's What You Need to Know About Australia's Coronavirus Tracking App', *ABC News* (online, 20 April 2020) https://www.abc.net.au/news/2020-04-20/how-will-australia-coronavirus-tracking-app-work/12163736.

[7]See Haran Burri and David Senouf, 'Remote Monitoring and Follow-Up of Pacemakers and Implantable Cardioverter Defibrillators' (2009) 11(6) *Europace* 701.

[8]See discussion in Kevin Warwick, 'The Cyborg Revolution' (2014) 8(3) *Nanoethics* 263. As to how a pacemaker would fulfil the traditional definition of cyborg, see Craig M Klugman, 'From Cyborg Fiction to Medical Reality' (2001) 20(1) *Literature and Medicine* 39, 42.

[9]See Maged Kamel Boulos et al, 'How Smartphones Are Changing the Face of Mobile and Participatory Healthcare: An Overview, With Example from eCAALYX' (2011) 10(24) *BioMedical Engineering OnLine* 1.

[10]*Telecommunications (Interception and Access) Act 1979* (Cth) ch 3 pts 3-1A, 3-2, 3-3, 3-5; ch 4 pt 4-1; ch 5 pts 5-1A.

[11]See *Privacy Act 1988* (Cth) sch 1 Australian Privacy Principles 3.4(d), 6.2(b), 6.2(e). See also proposed legislation in the Identity-Matching Services Bill 2019 (Cth).

[12]See George Williams, 'A Decade of Australian Anti-Terror Laws' (2011) 35(3) *Melbourne University Law Review* 1136.

[13]Australian Digital Health Agency, 'My Health Record Statistics' (February 2020). See also Christopher Knaus, 'More Than 2.5 Million People Have Opted Out of My Health Record', *The Guardian Australia* (online, 20 February 2019) https://www.theguardian.com/australia-news/2019/feb/20/more-than-25-million-people-have-opted-out-of-my-health-record.

[14]See, eg, *Public Health Act 2005* (Qld) ch 8 pt 2.

are safe. This has been the substance of a major government public relations campaign, with the Prime Minister declaring that the pubs will open if we download the app, and that we need to get the economy 'COVID-safe' to return to normal.[15]

Meow-Meow exercised his freedom to extend the functioning of his body by inserting the Opal card chip. But how free will we be from the requirement to extend our corporeal body through the incorporeal data contained in a contact tracing app? Without making the app mandatory, there are multiple ways that it might entrench itself within society to create classes of people based on their 'data status' as cyborgs: those whose provenance is known (via the app) and those whose provenance is not.

Clynes and Kline coined the term 'cyborg' in 1960 as a means of solving the problems of sending humans into space.

> For the exogenously extended organizational complex functioning as an integrated homeostatic system unconsciously, we propose the term 'Cyborg.' The Cyborg deliberately incorporates exogenous components extending the self-regulatory control function of the organism in order to adapt it to new environments.[16]

The term is most frequently associated with the notion of technoscientific enhancement of the human body. Clynes and Kline proposed a number of pharmacological interventions as answers to specific neurological and psychic challenges of space travel. While frequently appearing in dystopian science fiction, the cyborg, part human, part machine,[17] is encompassed within both trans-[18] and posthumanism,[19] augmented through embedded machines, gene editing, bodily enhancements, pharmacology, and other medico-technological means.

In a more radical departure from the mechanistic understanding of the cyborg, Haraway's iconic 1991 chapter engages with a more contemporary and far-reaching comprehension of the cyborg. For her, the 'cyborg myth is about transgressed boundaries, potent fusions, and dangerous possibilities . . .'[20] More akin to a broader posthumanist understanding of multiple intersections, Haraway uses the term to indicate fluidity between human–animal, human–machine, and human–information. Within this framework, therefore, she engages with 'a cyborg world [that] might be about lived social and bodily realities in which people are not afraid . . . of permanently partial identities and contradictory standpoints'.[21]

Of particular relevance to comprehending the data-enhanced individual as cyborg, Haraway observes that 'we are living through a movement from an organic, industrial society to a polymorphous, information system'[22] in which she describes new categories with the 'informatics of domination' including a shift from physiology to communications engineering.[23] This is part of her cyborg myth as the latter category, unlike the one it replaces, cannot be coded as natural.

Adopting Haraway's framework, we – individuals, citizens – are already cyborgs. We have enhanced ourselves and our social relations through close and almost ubiquitous engagement with information systems. In doing so, we have altered the boundaries between ourselves and the state[24] and corporations, as well as between each other. To the extent that information and its technologies support, drive, enhance, and inhibit our social interactions, we are already a society of cyborgs – despite our lack of consciousness of our status. Further, our consumption and governance, both part of our social relations, are similarly – and largely unconsciously – affected by our cyborg status.

The advent of COVID-19 and the race to manage the pandemic has brought our cyborg status to the fore. Discussion around contact tracing apps, in particular, is likely to awaken us to the possibilities and detriments that flow from humans being augmented in different ways: where we are differentiated by the extent to which we engage with and are absorbed by our data interfaces. This is our data status.

The COVID cyborg

The public health prescription for population-wide survival of the COVID-19 pandemic includes so-called social isolation, or physical distancing. In most jurisdictions this involves a combination of staying at home except for specified permitted activities,[25] and when away from home, remaining more than 1.5 m away from the next person.

In managing outbreaks of infectious diseases, public health practice involves tracing contacts of an infected person for the duration of the relevant incubation

[15]'Australia "on Track to COVID-safe Economy"', *Sky News* (online, 23 April 2020) https://www.skynews.com.au/details/_6151471990001.

[16]Manfred E Clynes and Nathan S Kline, 'Cyborgs and Space' (September 1960) *Astronautics* 26, 27.

[17]Gert Leonhard, 'Technology vs Humanity: The Coming Clash Between Man and Machine' (FutureScapes, 2016) loc1423 (kindle).

[18]Barbara Becker, 'Cyborgs, Agents, and Transhumanists: Crossing Traditional Borders of Body and Identity in the Context of New Technology' (2000) 33(5) *Leonardo* 361.

[19]Veronica Hollinger, 'Posthumanism and Cyborg Theory' in Mark Bould et al (eds), *The Routledge Companion to Science Fiction* (Routledge, 2009) 267.

[20]Haraway (n 3) 154.

[21]Ibid.

[22]Ibid 161.

[23]Ibid.

[24]Galloway (n 4).

[25]See, eg, *Home Confinement, Movement and Gathering Direction Qld* (2 April 2020).

period. A painstaking and tedious process, contact tracing depends upon the memory of the patient about people whom they have encountered during the couple of weeks preceding diagnosis. Public health authorities then contact those people for testing.

A number of jurisdictions have developed smartphone apps designed to facilitate the contact tracing process in the COVID-19 pandemic. In Australia, this is COVIDSafe. The Prime Minister has assured Australians that the app will not be mandatory. The government originally asserted that as a public health measure, the app required a 40 per cent uptake, population-wide, to have the desired effect of stopping outbreaks before they spread too far. It has since been revealed that this number is arbitrary, not based on any modelling.[26] It seems that government is hoping that Australians will voluntarily download and use the app as a means of cutting short the prescribed lockdowns and returning society to normal.

The app involves modification of the boundaries of ordinary human behaviour through the intercession of information. Those who download the app and carry their smartphone when leaving the house have extended their material being and the relations of their social interaction through data capture on their device, on devices of others in proximity who also carry the app, and ultimately to the public health authority. The Bluetooth signal, designed to be emitted to capture only prescribed interactions, is meaningless without its owner and the information identifying them. It is an extension, a modification, of the user's embodied self whose potential pathogenic transfer is of interest to the State. As Haraway observed nearly three decades ago,

> Human beings, like any other component or subsystem, must be localized in a system architecture whose basic modes of operation are probabilistic, statistical. No objects, spaces, or bodies are sacred in themselves; any component can be interfaced with any other if the proper standard, the proper code, can be constructed for processing signals in a common language.[27]

Each app user is interfaced with those they come in contact with, and the state, through the contact tracing app – which is designed to process the relevant signals in a common language. The user of the contact tracing app is the quintessential COVID cyborg.

Questions of data privacy aside, there are other interesting questions involving both the COVID cyborg, and those who choose not to upload the app, or who may not have access to the requisite device to be able to do so (called for these purposes 'app free'). The COVID cyborg, like Meow-Meow, will have chosen the path of modification. Unlike the case of Meow-Meow, however, government – and, it seems, broader society – is highly receptive to the social good apparently inherent in using the app. Conversely, while the unaugmented person was preferred to augmented Meow-Meow, with the contact tracing app it is possible that the app free person will not be so favourably regarded by broader society.

Over a week after the release of the COVIDSafe app, the Attorney-General released a Draft Exposure Bill.[28] As promised, the Draft Bill does not make the app compulsory. In addition to protection of the data collected, it contains a prohibition on requiring a person to download or use the app or to upload their data.[29] However, in light of the strong perception of public good attached to the app, there may be perceived social or financial imperatives for people to use it. Indeed, the first 10 days of the COVIDSafe app's operation saw examples of workplaces attempting to require employees to use the app to ensure that any potential spread of the disease is caught early. Employer groups have called for the right to require employees to download the app.[30] In a form of public shaming, opinion pieces started comparing those who are app free with anti-vaxxers,[31] and political analysis pieces published the app status of politicians with the implication that those who remained app free would hinder easing of COVID-19 restrictions.[32] In light of these attitudes, it is not difficult to imagine, for example, employers installing the app on work phones and requiring all work phones to run Bluetooth. This would effectively trace the employee, without engaging them in consent to use the app.

The recriminations against those who are app free in these scenarios reflect an understanding of a differential personal characteristic depending on one's data status, relative to whether they have uploaded or are using the app. Were this to be carried into our everyday interactions in employment or service delivery – regardless of the prohibition on coercion – the basis of discrimination is clearly outside existing grounds of discrimination law in Australia. If perceived as a qualifying factor for employment, or insurance, then although the Draft Exposure Bill proscribes coercion, it is difficult to see how the app

[26]'Coronavirus Tracing App COVIDSafe Hits 5 Million Downloads as Government Concedes Incompatibility with Older Phones', *ABC News* (online, 6 May 2020) https://www.abc.net.au/news/2020-05-06/coronavirus-covidsafe-5-million-download-officials-concede-flaws/12221004.

[27]Haraway (n 3) 163.

[28]Privacy Amendment (Public Health Contact Information) Bill 2020. The Bill received Royal Assent on 15 May 2020.

[29]Proposed s 94H.

[30]Ewin Hannan and Stephen Lunn, 'Employers want Power over App', *The Australian* (Sydney, 7 May 2020) 5.

[31]Angela Mollard, 'People Who Refuse to Download the COVIDSafe Virus Tracing App Are the New Anti-vaxxers', *News.com.au* (6 May 2020) https://www.news.com.au/world/coronavirus/australia/people-who-refuse-to-download-the-covidsafe-virus-tracing-app-are-the-new-antivaxxers/news-story/541c36fe5cdb56eb1a098b0b9a0dddcc.

[32]'Easing Coronavirus Restrictions Depends on the Uptake of the Government's Tracing App, so has your MP Downloaded It?' *ABC News* (online, 7 May 2020) https://www.abc.net.au/news/2020-05-07/has-your-mp-downloaded-the-coronavirus-tracing-app/12215092?nw=0.

free person might usefully challenge such discrimination. For while the analysis here regards the user as a cyborg, this is not currently a category known to law – a point made by Meow-Meow.

Considering what is perceived to be an inevitable convergence of human and technology, scholars such as Gray[33] have suggested the need to address the legal issues it will raise – notably in terms of rights. Gray has formulated 10 amendments to the US Bill of Rights as a way of framing what he sees as the core issues facing cyborgs. The questions raised here relate not to the need to protect cyborgs per se, but rather the possible need to protect choices that we make in terms of our data status – notably any requirement to become a COVID cyborg. Further, protections need to extend both in terms of interactions with the State and in social and business engagements. In other words, the protections need to be as broad as possible, beyond the simple prohibition on coercion contained in the Draft Exposure Bill.

If the app remains voluntary but gains social acceptance, as seems likely, then there is a strong argument that those who are app free may be afforded less favourable treatment in diverse contexts. Five of Gray's 10 human rights statements provide guidance as to how such protections might be framed – albeit framed in the negative to his positive statements of cyborg rights.

First, cyborgs should have 'freedom of electronic speech'. Gray extends this to include 'non-physical forms of transmitting information'.[34] The person who remains app free, on the other hand, and with the contact tracing app in mind, should have freedom *from* electronic speech. If the app is to be voluntary, then the organic person must be under no compulsion to use it. Expressing this as a substantive right aims to capture social pressures and indirect requirements illustrated above.

Second is the 'right of electronic privacy'.[35] Unlike freedom of electronic speech, this might apply equally to COVID cyborgs and those who are app free. Intended to fall within the US Fourth Amendment protection against unwarranted searches and seizures, the right might apply so that a person could not be required to disclose their status under the contact tracing app. By these means, an employer, or insurer, would be prohibited from asking for evidence of having signed up to the app as a precondition of employment or a claim. One's status as an app user is itself private information, and not open to interrogation.

Third is the 'right to life'.[36] Gray argues that the body of the citizen should not only be protected against interference, but that the individual should retain the right to modify their body 'through psychopharmacological, medical, genetic, spiritual and other practices . . . '.[37] In terms of body modification, this has been described more specifically as a right to bodily integrity. Relevantly to this argument, bodily integrity comprehends the integration of the self and the rest of the objective world.[38] Accordingly, Gray's interpretation of the right to bodily integrity might extend to modification through information communication. Indeed, it is a premise of this article that engaging with information practices is a bodily modification that should be included in these categories. Embraced within the right to life, as with the first right, this should be framed to protect a person's right to refuse to modify their body by adopting information practices demanded by the app.

Fourth is the right to political equality.[39] This too needs no alteration from the original but is to be read so that regardless of one's cyborg status, they hold this right. Including this right recognises the political nature of governmentality of the body.[40] Regardless of legislative prohibition on coercion regarding COVIDSafe, if the app and its information are integral to one's body, then the app is an exercise of biopower. Given the broader social context of the app (illustrated above), its adoption represents the socialisation of biopower including the exercise of sovereign power. To refuse to download or use the app might, in this sense, represent a political act. Where those who remain app free are persecuted for this stance should be protected for what might be

[33]Gray (n 2).
[34]Gray's second amendment: ibid 27.
[35]Gray's third amendment: ibid 28.
[36]Gray's fifth amendment: ibid.
[37]Ibid.
[38]Jonathan Herring and Jesse Wall, 'The Nature and Significance of the Right to Bodily Integrity' (2017) 76(3) *The Cambridge Law Journal* 566.
[39]Gray's seventh amendment: Gray (n 2) 28.
[40]Maurizio Lazzarato, 'From Biopower to Biopolitics' (2002) 13(8) *Pli: The Warwick Journal of Philosophy* 1.

construed as political speech. In the Australian context, political equality exists in the form of an implied right to freedom of political communication.[41] Under this fourth right, if a refusal to use the app is political communication it should constitute a protected action.

Finally, is freedom of information.[42] Importantly in the context of COVID-19, this right provides that it is 'absolutely forbidden' for an institution or corporation to use information to 'coerce or illegally manipulate or act upon' a citizen.[43] The converse of this, for protection of those who are app free, is to forbid acting upon the fact that such information is absent. This would extend even to inquiring as to one's app status (whether you had downloaded it or not).

Importantly, Gray's framework has an overarching goal of protecting cyborgs from 'relentless change' wrought by 'Cyborgian technoscience'.[44] A more broadly derived scope of protections might apply not only to those who modify themselves (or who are otherwise modified) but those who choose not to.

In sum, a human rights framework offers the scope to comprehend cyborgs as equal before the law, regardless of the extent of their body modification choices.

Conclusion

As public health officials, governments, and citizens generally are grappling with a radically changed environment due to COVID-19, it is to be expected that society will employ an array of solutions to deal directly with the pandemic, and also its aftermath. Some will appear new because of the novel and unfamiliar context. Thus, although smartphones and the app ecosystem has been widespread for many years now, the notion of an ever-present app designed to record contacts for public health purposes is new.

Although, on one analysis, humans have inevitably already crossed over into the realm of cyborg, the contact tracing app provides a new context that brings into relief the idea of an enhanced human. Despite the urgency of rolling out attempts to solve the COVID lockdown, in another sense we have the luxury, finally, of considering the downstream implications of this kind of solution because of the particular circumstances of its development and implementation.

Through this thought experiment – adopting perhaps a somewhat unfamiliar categorisation of the technology – and adapting existing thinking surrounding individual rights, the conclusion is one that might have been anticipated all along. Close consideration to a bill of rights that encompasses not only questions of privacy, but also an extended comprehension of the human, may support the development of an infrastructure within which we can safely add tools that will serve the public good, while limiting the obvious risks.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD


Kate Galloway https://orcid.org/0000-0002-8047-1210

Kate Galloway is an Associate Professor in the Griffith Law School at Griffith University.

[41] *Lange v Australian Broadcasting Corporation* (1997) 145 ALR 96, 112; *Coleman v Power* (2004) 209 ALR 182, 232-3. See discussion in Leanne Griffiths, 'The Implied Freedom of Political Communication: The State of the Law Post Coleman and Mulholland' (2005) 12(1) *James Cook University Law Review* 93.

[42] Gray (n 2) 28.

[43] Ibid.

[44] Ibid 29.