Received: 19 June 2020 | Revised: 25 October 2020 | Accepted: 12 January 2021

DOI: 10.1111/bioe.12856

COVID-19

bioethics WILEY

Ethics, public health and technology responses to COVID-19

Seumas Miller[1,2,3] | Marcus Smith[1]

[1]Charles Sturt University, Canberra, Australia

[2]TU Delft, The Hague, Netherlands

[3]University of Oxford, Oxford, UK

Correspondence
Seumas Miller, Charles Sturt University, Canberra, Australia.
Email: semiller@csu.edu.au

ABSTRACT

The COVID-19 pandemic has infected millions around the world. Governments initially responded by requiring businesses to close and citizens to self-isolate, as well as funding vaccine research and implementing a range of technologies to monitor and limit the spread of the disease. This article considers the use of smartphone metadata and Bluetooth applications for public health surveillance purposes in relation to COVID-19. It undertakes ethical analysis of these measures, particularly in relation to collective moral responsibility, considering whether citizens ought, or should be compelled, to comply with government measures.

KEYWORDS

collective responsibility, coronavirus, COVID-19, privacy, public health, surveillance, technology

1 | INTRODUCTION

The coronavirus (COVID-19) pandemic has impacted countries around the world, resulting in a large number of infections and deaths, requiring citizens to self-isolate, and causing a severe contraction in the global economy. While most individuals that are infected only experience mild respiratory illness, for the elderly and those with underlying medical conditions, it is life threatening. Protecting populations has required businesses to cease trading, social distancing measures, the closure of schools, and the implementation of work from home policies. Despite these measures, by October 2020, COVID-19 had infected more than 40 million people around the world and killed more than one million.[1] The situation in the United States, where more than 200,000 have died, has been complicated by gatherings, large protests and rioting across the country, e.g. some associated with the Black Lives Matter movement,[2] others with right wing groups, anti-lockdown protests, and President Trump's political rallies (at which masks have typically not been worn).

As governments implemented biosecurity powers to force compliance with the business closures and social distancing measures, available technologies were deployed to ensure adherence with new laws, and conduct contact tracing of those who contracted COVID-19. The use of phone metadata, as police might often do after obtaining a warrant in a criminal investigation, to geo-locate individuals and track their movements, occurred in liberal democracies as the seriousness of the pandemic intensified. Phone applications were subsequently introduced by governments in a number of countries that communicate with surrounding phones via Bluetooth to record other persons that an individual has been in close contact with, and some employed GPS tracking.

The development of technology over the past two decades has enhanced the capacity to obtain and share data. COVID-19 represents a serious threat to life and well-being in the community where the use of all available data may be justified, but consideration must also be given to ethical implications such as individual autonomy and privacy. There are strong public policy reasons to use available technology to limit the spread of diseases such as COVID-19 that have the capacity to inflict profound impacts on society. However,

[1]World Health Organisation. (2020). *Coronavirus disease (COVID-2019) situation reports*. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports

[2]Taylor, D. B. (2020, May 30). George Floyd protests: A timeline. *New York Times*. https://www.nytimes.com/article/george-floyd-protests-timeline.html

it is also important that this occurs appropriately, and that public acceptance of surveillance in extraordinary situations does not lead to normalization once the situation has been resolved.

This article is organized into four parts. Part 2 focuses on technology responses to mitigate the spread of the pandemic. It discusses the use of government sanctioned smartphone applications, and metadata, to track citizens that have COVID-19, or may have been exposed. Part 3 undertakes an ethical analysis of the government response to COVID-19. The article concludes by applying the concept of collective responsibility to the technology responses implemented by governments in response to the COVID-19 pandemic.

2 | TECHNOLOGY RESPONSES

Presented with the serious threat of COVID-19, governments were forced to take radical action to limit the spread of the disease, including making full use of available technologies. Emergency public health powers exist for these contingencies and allow for actions to be taken that would be unimaginable under normal circumstances.[3] These measures—including travel bans, closing businesses and quarantine—could potentially be misused and transform a liberal democracy into an authoritarian state. However, governments have an obligation to reduce harm and protect their citizens from an imminent threat.

The protests and gatherings described above, have taken place across many cities in the United States and around the world. In some locations, such as Washington D.C. and New York, tens of thousands congregated in public areas in defiance of social distancing orders. While exercising the democratic rights and expressing legitimate concerns about social inequality, this presented some public health concern.[4] There is a legitimate need for governments to identify individuals that may either have COVID-19, have been exposed to someone who has COVID-19, or have been directed to self-isolate for a period of time and not leave a residence or hotel. In the context of these demonstrations, it could be necessary to identify participants for public health reasons in order to prevent a second wave of infection that could kill tens of thousands.

Governments around the world use available technology to identify individuals for identification purposes. Law enforcement agencies have been involved in enforcing COVID-19 laws that restrict movement or close a business, and have a range of surveillance technologies available to them. These include closed-circuit television cameras, metadata access, automated numberplate recognition, financial transaction and GPS tracking.[5] Two approaches will be examined in this discussion—smartphone metadata, and applications that use Bluetooth technology to communicate with phones in their vicinity, rather than track users' locations. GPS tracking applications have not been widely pursed due to significant privacy concerns. In Norway, where the government application did employ GPS tracking, its operation was suspended.[6]

2.1 | Bluetooth applications

In March 2020, the Singapore Government launched a smartphone application to assist in monitoring COVID-19 by enabling public health authorities to investigate infections and limit further transmission. In May 2020, the Australian Government announced it was implementing similar technology.[7] These apps use Bluetooth technology to communicate between phones rather than location metadata, and for this reason were promoted as having a low impact on individual privacy. It sought to incentivize its use by highlighting that if this take-up was achieved, social restrictions could be safely eased: 'We need that tool so that we can open up the economy…that's why it's so important'.[8] In less than a month over six million people had downloaded the app.[9]

The benefit of this technology is that it does not use metadata or GPS, but communicates with surrounding phones using Bluetooth technology, recording those (which have downloaded the application) that have been in close proximity for a minimum time period. The data is held for a period of time and is then deleted. It therefore does not monitor an individual's location: only their phone's relationship to other phones. It is irrelevant where a person was when they were in close proximity to another person that subsequently tested positive for COVID-19, only that they were at some point close enough to be infected. The data is only decrypted and accessed by public health officials once a person tests positive—and then only consists of the phone numbers of others they have been in close proximity to, enabling them to be

[3]For example, on March 18, 2020, the Australian Government declared a human biosecurity emergency under provisions of the *Biosecurity Act 2015* (Cth). This provides expansive powers for a three month human biosecurity emergency period, when the Minister is authorized to issue any direction, or establish any requirement they consider necessary to prevent or control the spread of COVID-19. Similar powers exist in the United States for the Secretary of Health and Human Services, and the President, under the *Public Health Service Act* (Pub.L. 78–410), the *Constitution* and the *National Emergencies Act*. (Pub.L. 94–412).

[4]Goldberg, E. (2020, 7 June). George Floyd protests add new front line for coronavirus doctors. *New York Times*. https://www.nytimes.com/2020/06/07/health/doctors-george-floyd-coronavirus.html

[5]Servick, K. (2020, 21 May). COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work? *Science*. https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-containcoronavirus-how

[6]Ibid.

[7]Bogle, A. (2020, 27 April). Will the government's coronavirus app COVIDSafe keep your data secure? Here's what the experts say. *Australian Broadcasting Corporation News*. The Australian Government did not require citizens to download the application, but initially stated that 10 million people (40 percent of the population) would need to download it in order for it to function effectively. https://www.abc.net.au/news/science/2020-04-27/covidsafe-contact-tracing-app-coronavirus-privacy-security/12186044

[8]Australian Broadcasting Corporation News. (2020, 1 May). *The main points from Scott Morrison's latest coronavirus update*. https://www.abc.net.au/news/2020-05-05/morrison-key-points-on-coronavirus-economic-response/12217026

[9]Australian Broadcasting Corporation News. (2020, 24 May). *Coronavirus Australia news: 6 million people have now downloaded the COVIDSafe tracing app*. https://www.abc.net.au/news/2020-05-24/coronavirus-australia-live-news-covid-19-latest/12280370

contacted and tested. If the application functions as described, it would appear to mitigate the privacy concerns associated with metadata—noting of course that under the emergency public health powers that have been implemented, the government could still access an individual's metadata for a COVID-19 purpose if it was deemed necessary.

Bluetooth applications have been associated with varying levels of functionality, depending on: whether a phone is locked or unlocked; whether the communicating phones utilize Android or iOS operating systems; and the degree of interference between the phones, such as the number of people standing between them.[10] For instance, after a month of use, and despite ongoing updates to address these issues, some Bluetooth applications in Singapore and Australia were only performing at a moderate level with regard to locked phones using iOS.[11] In considering the ethical implications of these technologies, performance and efficacy must be considered as part of an evaluation of whether the benefits of the application outweigh costs such as privacy risks, as well as in relation to alternatives.

2.2 | Metadata

Metadata refers to information such as the location of the devices used, the phone numbers involved in a communication, and the date and time of the communication.[12] It includes location data because a smartphone is regularly in contact with nearby cell towers to maintain reception. For these reasons, metadata can provide a detailed picture of an individual's movements, particularly when this data is analysed over periods of time.

The COVID-19 pandemic has brought to light another use for phone metadata—contact tracing and public health order enforcement. Almost as soon as governments implemented social isolation and distancing requirements, smartphone metadata was being used around the world to track the location of individuals who have been diagnosed with COVID-19. It can assist in identifying people that a person may have had contact with, as well as to track those who have been required by law to self-isolate. While limited examples are on the public record, it has been reported that police have accessed the metadata of individuals known to be infected with COVID-19, in order to identify which locations they had visited, and people they had been in contact with. They confirmed that the same systems were used to access metadata for this purpose as those in a criminal investigation if a threshold is met regarding suspicion of a serious offence. Their view was that COVID-19 placed the community at risk of life-threatening consequences and that this warranted access to metadata: 'In this case, we think there's a genuine risk to public safety, and certainly there's community concern about this, so it's one of the occasions we elected to use it'.[13]

In South Korea, the government has relayed individuals' metadata information to the community in public health messaging. The government published anonymized data of the locations that individuals who have tested positive to COVID-19 had visited, including sending text messages to citizens residing in a specific locality. For instance: 'A woman in her 60s has just tested positive. Click on the link for the places she visited before she was hospitalised'.[14] Depending on the population size of the locality, the specificity of these messages may allow those individuals to be identified.

In Israel, the government has approved emergency regulations that give authorization for Shin Bet, the internal security agency, to utilize a previously undisclosed database to track the movements of individuals that test positive for COVID-19, and identify those that they are likely to have had contact with:

> The use of advanced Shin Bet technologies is intended for one purpose only: saving lives, in this way, the spread of the virus in Israel can be narrowed, quickly and efficiently. This is a focused, time-limited and limited activity that is monitored by the government, the attorney general and … regulatory mechanisms.[15]

The availability of location metadata for use in relation to the COVID-19 epidemic in 2020 is a result of technological, political and legal developments over the past 20 years. From 9/11 onwards, in the United States, the United Kingdom and other liberal democratic countries, the threat from terrorism resulted in a number of significant changes to legislation and practices of law enforcement and security agencies.[16] In many countries, telecommunications providers are now required to retain their customers' metadata for a number of years to ensure it is available if it is subsequently needed for a law enforcement or other government purpose.[17] More broadly, the net result of these reforms is that governments have provided these agencies much greater powers to collect evidence and conduct surveillance, and to do so more proactively, in order to detect and counter elusive non-state threats like terrorism and transnational crime. The impact of these

[10]Bogle, A. (2020, 17 June). COVIDSafe app tests revealed iPhone performance issues at launch that weren't shared with the public. *Australian Broadcasting Corporation News*. https://www.abc.net.au/news/science/2020-06-17/covidsafe-contact-tracing-app-test-documents-rated-poor-iphone/12359250

[11]Ibid.

[12]Walsh, P., & Miller, S. (2016). Rethinking 'five eyes' security intelligence collection policies and practice post Snowden. *Intelligence and National Security*, *31*, 345–368, 351.

[13]Sutton, M. (2020, 6 February). Phone tracking used to follow movements of Chinese couple with coronavirus in Adelaide. *Australian Broadcasting Corporation News*. https://www.abc.net.au/news/2020-02-06/phone-tracking-follows-movements-of-couple-with-coronavirus/11935912

[14]Kim, N. (2020, 6 March). More scary than coronavirus: South Korea's health alerts expose private lives. *The Guardian*. https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives

[15]Halbfinger, D., Kershner, I., & Bergman, R. (2020, 16 March). To track coronavirus, Israel moves to tap secret trove of cellphone data. *New York Times*. https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html

[16]Ibid, 354. [from Walsh & Miller]

[17]See e.g. in Australia, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) came into effect in October 2015. The data that telecommunications service providers are required to retain is outlined in section 187AA.

changes initiated debates about whether this more proactive collection of data, from citizens who have not committed a crime is acceptable, and on the ethics of information collection programs more generally.[18]

The country where COVID-19 originated, China, is the world leader in public surveillance.[19] China's social credit system uses data integration with the capacity to create a detailed picture of an individual's life and impose sanctions on citizens, such as restricting access to transport systems, if they repeatedly fail to comply with social norms. Its systems integrate facial recognition with a widespread public CCTV network and almost all other forms of available data to monitor its citizens.[20] Governments in all developed countries now have the capacity to link databases of biometric templates, CCTV footage, phone and email metadata, as well as financial, medical and other records. The public health emergency powers enacted in liberal democracies during the COVID-19 pandemic allow them to operate to some extent like an authoritarian government and arguably create a power imbalance between the government and its citizens. The following part of the paper will discuss the ethical considerations associated with this aspect of governments' technology response to the COVID-19 pandemic.

3 | ETHICAL CONSIDERATIONS

The use of surveillance technologies by government raises a number of pressing ethical concerns for liberal democracies.[21] In the public health context of COVID-19, the concerns relate especially to the potential conflicts between biosecurity, on the one hand; and individual privacy and autonomy, and democratic accountability, on the other.[22] Biosecurity, and associated public health and safety, are fundamental values in liberal democracies, as in other polities, including many authoritarian ones. However, liberal democracies are also committed to individual privacy and autonomy, democracy, and therefore, democratic accountability.

Moreover, as recent economic lockdowns and protests illustrate, public health considerations may conflict with (individual and collective) autonomy, including the right to freedom of movement, the right to buy and sell goods, and the right to (peacefully) protest. Accordingly, the latter fundamental privacy and autonomy rights must continue to be valued in liberal democracies, notwithstanding the importance of public health and the contribution that surveillance technologies in particular (in conjunction with social distancing measures, quarantine requirements and, perhaps, lockdowns and prohibitions on public protests) can provide to maintain it. While debates will continue between proponents of security, on the one hand, and defenders of privacy, on the other, there is often a lack of clarity in relation to the values or principles allegedly in conflict. Moreover, a principle that lies at the heart of these debates has not received the attention it warrants, namely, the collective moral responsibility to ensure security and public health.

3.1 | Security and public health

The notion of security is somewhat vague. Sometimes it is used to refer to a variety of forms of collective security, for example national security (such as harm to the public from a terrorist attack), community security (such as in the face of disruptions to law and order posed by violent political demonstrations) and biosecurity (such as threats to public health and society caused by COVID-19). At other times it is used to refer to personal physical security. Physical security in this sense is security in the face of threats to one's life, freedom or personal property—the latter being goods to which one has a human right.

Personal (physical) security is a more fundamental notion than collective security; indeed, collective security in its various forms is in large part derived from personal security. Thus COVID-19, for example, is a threat to public health and national security precisely because it threatens the lives of individual citizens. However, collective security is not simply aggregate personal (physical) security. For example, COVID-19 might be a threat to the stability of a government and, as such, a national security threat.

Arguably, security should be distinguished from safety, although the two concepts are related and the distinction somewhat blurred. We tend to speak of safety in the context of natural disasters, pandemics and the like in which the harm to be avoided is not intended harm. By contrast, the term 'security' typically implies that the threatened harm is intended. At any rate, it is useful to at least maintain a distinction between intended and unintended harms and, in relation to unintended harms, between foreseen, unforeseen and unforeseeable harms. For instance, someone who is unknowingly carrying the COVID-19 virus because they are asymptomatic, is a danger to others but, nevertheless, might not be culpable (if, for instance, they had taken reasonable measures to avoid being infected, had an intention to test for infection if symptoms were to arise and, if infected, would take all possible measures not to infect others).

There is an existing body of literature on security that acknowledges the way it can be used politically to 'make socially effective claims about threats'[23] and position an issue as a threat to survival that 'enables emergency measures and the suspension of 'normal politics' in dealing with that issue.'[24] It has been argued that labelling

[18]Henschke, A. (2017). *Ethics in an age of surveillance*. Cambridge University Press.

[19]Qiang, X. (2019). The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy, 30*, 53–67.

[20]Ibid.

[21]Kleinig, J., Mameli, P., Miller, S., Salane, D., & Schwartz, A. (2011). *Security and privacy*. ANU Press.

[22]Biosecurity will be defined as public health measures seeking to prevent the introduction and spread of harmful organisms (viruses, bacteria), to minimize the risk of transmission of infectious diseases to people.

[23]Williams, M. (2003). Words, images, enemies: Securitization and international politics. *International Studies Quarterly, 47*, 511–531, 514.

[24]McDonald, M. (2008). Securitization and the construction of security. *European Journal of International Relations, 14*, 563–587, 567.

an issue one of security, allows exceptional actions to be taken beyond what would normally be politically acceptable, and that '[an] issue becomes a security issue … not necessarily because a real existential threat exists but because the issue is presented as a threat'.[25]

Kamradt-Scott and McInnes (2012) have observed that pandemics have previously been used by governments to move outside of 'normal politics':

> The effect of framing pandemic influenza as a threat to national and international security has, however, been profound both in terms of measures undertaken and the global spread of responses. Most states, as well as key international institutions, have reacted to the construction of pandemic influenza as a threat by establishing emergency planning measures, which take responses to the disease outside the realm of 'normal politics'. In this respect, the successful framing of the disease as a security issue opened up a pathway for exceptional responses.[26]

In implementing exceptional responses to pandemics it is important that governments act ethically. Parker et al. (2020) argue that a requirement of 'public health interventions to address the threat of COVID-19 will be recognition of the importance of engaging seriously with equity and justice issues'.[27] If governments fail to do so, this can have implications in terms of the trust of the community in relation to future public health intervention and public policy more broadly. Ranisch and Nijsingh (2020) discussed the importance of government maintaining trust of the community COVID-19 contact tracing apps:

> Trust is essential in public health decision-making in general, and COVID-19 CT apps in particular … Well-founded trust requires taking seriously the ethical complexities relating to the implementation of CT apps as well as being transparent about the inevitable trade-offs that are being made. Communicating goals and functions as well as possible benefits, risks, and limitations of CT apps clearly and early can play a crucial role in preventing squandering trust and misconceptions.[28]

Ethical problems arise from the expanding use of metadata for COVID-19 public health surveillance and for other security purposes, especially in the context of interlinkage with other data available to governments, such as biometrics, and associated rapidly developing data analytics and artificial intelligence capabilities. First, the security contexts in which their use is to be permitted might become both very wide and continuing, e.g. the COVID-19 ('biosecurity emergency') context becomes the need to prevent future pandemics and maintain public health more generally; just as, arguably, the 'war' (without end) against terrorism became the war (without end) against serious crime; which, in turn, became the 'war' (without end) against crime in general. Second, data, including surveillance data, originally and justifiably gathered for one purpose, e.g. taxation or combating a pandemic, is interlinked with data gathered for another purpose, e.g. crime prevention, without appropriate justification. The way metadata use has expanded in some countries, from initially being used by only a few police and security agencies to being used quite widely by governments in many western countries, is an example of function creep and illustrates the potential problems that might arise as the threat of COVID-19 eases.[29] Function creep is a significant and growing problem associated with the regulation of technology. If liberal democratic governments are to maintain the trust of the community, data collected for one purpose, particularly to address an extraordinary circumstance, and which has been collected in a manner that may not otherwise have been acceptable, must be carefully guarded and not used for broader purposes.[30] The potential use of surveillance technologies, and the associated large-scale violations of privacy and autonomy rights is illustrated by the extensive social credit system established in China, described above, and in particular its use to monitor ethnic minorities.[31]

3.2 | Collective responsibility

As we have seen, the provision of more specific information to the community in response to the pandemic as South Korea has done, can be contrasted with the initial approach of extensive lockdowns that have been implemented in Europe, the United States and Australia and, of course, quarantine, enforced lockdowns and the like compromise individual autonomy. However, arguably, the *collective moral responsibility*[32] to combat the pandemic overrides individual autonomy rights (albeit restrictions on autonomy, such as lockdowns, also have deleterious economic effects).

Evidently, strategies for combating COVID-19 involve a complex set of often competing, and sometimes interconnected moral considerations (e.g. some privacy rights, such as control over personal data, are themselves aspects of autonomy); so hard choices have to be made. However, the idea of a collective responsibility on the part of individuals to jointly suffer some costs, e.g. loss of privacy

[25]Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner, 24.

[26]Kamradt-Scott, A., & McInnes, C. (2012). The securitisation of pandemic influenza: Framing, security and public policy. *Global Public Health*, *7*, 95–110, 106.

[27]Parker, M., Fraser, C., Abeler-Dorner, L. & Bonsall, D. (2020). Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. *Journal of Medical Ethics*, *46*, 427–431, 430.

[28]Ranisch, R., & Nijsingh, N. (2020). *Ethics of digital contact tracing apps for the COVID-19 pandemic response*. Technical Report, Competence Network Public Health COVID-19, 13.

[29]Smith, M., & Urbas, G. (2020). *Technology law*. Cambridge University Press.

[30]Ibid.

[31]Qiang, op. cit. note 19.

[32]Miley, M. (2017). Collective responsibility. In E. N. Zalta (Ed.), *The Stanford encyclopaedia of philosophy*. https://plato.stanford.edu/entries/collective-responsibility/; Bazargan-Forward, S., & Tollefsen, D. (Eds.) (2020). *The Routledge handbook of collective responsibility*. Routledge.

rights, in favour of a collective good (eliminating or containing the spread of COVID-19) lies at the heart of all such effective strategies. Accordingly, we need an analysis of the appropriate notion of collective responsibility.

One of the central senses of collective responsibility is responsibility arising from joint actions (and joint omissions). Roughly speaking, a joint action can be understood thus: two or more individual persons perform a joint action if each of them intentionally performs his or her individual action but does so with the (true) belief that in so doing each will do their part and they will jointly realize an end that each of them has and that each has interdependently with the others i.e. a collective end.[33] On this view of collective responsibility as joint responsibility, collective responsibility is ascribed to individuals;[34] moreover, if the joint action in question is morally significant, e.g. by virtue of the collective end being a collective good or a collective harm, then the individuals are collectively *morally* responsible for it. Each member of the group is individually responsible for his or her own contributory action, and (at least in the case of most small-scale joint action) each is also individually (fully or partially) responsible for the aimed at outcome, i.e. the realized collective end, of the joint action. However, each is individually responsible for the realized collective end, *jointly with the others*; hence the conception is relational in character. As already mentioned, if the collective end of the joint action is a collective good or a collective harm, then these individual persons are collectively morally responsible for this good or harm.

Here we need to make a number of important points. Firstly, this account of collective responsibility as joint responsibility pertains not only to joint actions but also to joint *omissions*, e.g. cases in which members of a group decide not to jointly act to avoid a harm to themselves or others. Secondly, it is possible that while each participant in a morally significant joint action makes a causal contribution to the aimed at outcome of the joint action, none of these contributing actions considered on its own is either necessary or sufficient for this outcome; this is especially so in the case of large-scale joint actions involving large number of participants. Thirdly, large-scale morally significant joint actions and omissions, such as fighting the COVID-19 pandemic, introduce a range of issues that are often not present in small-scale, morally significant joint actions and omissions. For one thing, large-scale cases often involve hierarchical organizations and hence the potential for those in subordinate positions having diminished moral responsibility. For another thing, the extent of the contribution to the outcome of a joint action or omission can vary greatly from one participant to another, e.g. one person might contribute by staying at home while another is a front-line health worker. Indeed, some of those who make a causal contribution to a joint action—and especially to large-scale joint actions—might, nevertheless, not be genuine participants in that joint action because in performing their contributory action they were not aiming at the outcome constitutive of the joint action; that is, did not have its collective end as their end.

Let us now apply this concept of collective moral responsibility to the COVID-19 pandemic and, in particular, to the use of phone applications to combat the pandemic. The use of one or more of these applications involves, let us assume, a moral cost to each individual in terms of his or her privacy since, for instance, his or her movements are being tracked (and there is the possibility that this location data will be misused by the government). However, there is a collective good to which, let us assume, the use of one or more of these applications can make a significant contribution, namely, the preservation of the lives of those who would otherwise have died as a result of the pandemic. Naturally, those whose lives would not have otherwise been preserved receive a benefit, namely, their life, that those who would have survived had they been infected do not receive. However, it is by no means certain who would survive being infected and who would not. Moreover, the death of large numbers of the members of a community as a result of a pandemic imposes personal and economic costs on those who survive the pandemic. Further, and most importantly, the survival of a large number of the members of a community is surely a good of such magnitude that it outweighs the privacy costs imposed on the members of the community. It clearly outweighs the privacy cost to each individual, including those who would survive even if infected.[35] Moreover, it also outweighs the aggregate privacy costs of the members of the community.

And there is this further point in relation to the greater costs that might be imposed on some members of the community than on others in relation to COVID-19. Here the notion of a web of interdependence is salient.[36] In any community there is a complex structure of direct, and indirect, synchronic and diachronic, interdependence (as opposed to mere one-way dependence) and overlap between the needy and those who fulfil their needs. For example, there is direct interdependence between police and citizens, employers and employees, farmers and consumers of their produce; and there is indirect interdependence between health-workers and their patients, given patients can include members of all of the above groups. Moreover, the interdependence is diachronic in so far as the older generation is now dependent on the younger and the younger was dependent on the older, and so on.

This web of interdependence is, of course, not of such a kind that the meeting of the needs of a single person is a necessary or sufficient condition for the meeting of the needs of any other single person, let alone of all other persons taken in aggregate.

[33]Miller, S. (1992). Joint action. *Philosophical Papers*, *21*(3), 275–297; Miller, S. (1995). Intentions, ends and joint action. *Philosophical Papers*, *24*(1), 51–67; Miller, S. (2007). Joint action: The individual strikes back. In S. Tsohatzidis (Ed.), *Intentional acts and institutional facts* (pp. 73–92). Springer.

[34]Miller, S. (2006). Collective moral responsibility: An individualist account. *Midwest Studies in Philosophy*, *30*(1), 176–193.

[35]Giubilini, A., Douglas, T., Maslen, H., & Savulescu, J. (2018). Quarantine, isolation and the duty of easy rescue in public health. *Developing World Bioethics*, *18*, 182–189. As these authors point out, the argument here is not a simple consequentiality cost/benefit analysis. They also point out that the duty to assist might remain even if the costs borne are quite high as long as they are relatively low compared to the harm prevented.

[36]Miller, S. (2010). *The moral foundations of social institutions: A philosophical study* (pp. 70–76). Cambridge University Press. Miller, S. (2019). *Institutional corruption: A study in applied philosophy* (pp. 40–45). Cambridge University Press.

Rather the interdependence between individuals, between small subsets of the whole community, and between individuals and small subsets is partial and incremental. Roughly speaking, the larger the subset, the greater the dependence on it of its members (taken individually) and of individuals and subsets outside it; and the less dependent it is on any particular subset outside it (or on any small subset of itself).

This de facto web of interdependence undermines the proposition that those who are not vulnerable to COVID-19 only have moral obligations to those who are vulnerable by virtue of the needs of the latter. For the former also have needs, even if not current needs for health protection from COVID-19, and these past, present or future needs, e.g. for an education (in the past) or for present or future employment in a tourist sector decimated by COVID-19, are or will be met, or have been met in the past, directly or indirectly, by members of the latter. In short, the web of interdependence generates reciprocal moral obligations among members of a community and these obligations obviously include obligations to preserve the lives of other members of the community, if in doing so they do not incur significant costs.[37]

Other things being equal, and assuming that the phone application(s) in question are effective, there is a collective moral responsibility on the part of members of the community confronting the pandemic to download a Bluetooth application and act accordingly. Of course, other things might not be equal. For instance, the data made available to authorities might be misused. Moreover, the set of persons who are collectively morally responsible might not include all the members of the community, e.g. those who are unable to use a smartphone or who cannot afford one should be excluded.

Notice that, as mentioned above, this conception of collective responsibility as joint responsibility implies that each relevant person has an individual moral responsibility to download a Bluetooth application (assuming the others do). So it is not simply a matter of whether each wants to do so; rather each has a moral obligation to comply (given the others comply). However, it does not follow from this that each should be compelled to comply; it does not follow that compliance should be a matter of enforceable law. On the other hand, if the numbers who choose to comply under circumstances in which compliance is voluntary, is not sufficient to enable a Bluetooth application to be effective, then it may well be that compliance ought to be enforced by the state. For the magnitude of the evil to be avoided outweighs any given individual's autonomy in respect of using the application (as well as his or her privacy) and, indeed, the aggregate autonomy (and privacy) in respect of using the application. Moreover, the moral weight attached to the reciprocal obligations generated by the web of interdependence can also be placed on the scale in favour of enforced compliance by the state.

And there is this further point. Given the questions about the functionality of Bluetooth applications and the seriousness of the threat posed by COVID-19, governments may need to resort to an option more invasive of privacy, such as analysis of metadata; and compliance with this option might need to be enforced. Perhaps—depending on the extent of the COVID-19 infection and the number of lives at risk—this should only be done in specific cases where individuals known to have the disease have placed others in the community at risk. If so, then greater, yet morally justified, moral costs (privacy and associated autonomy costs) would be imposed on members of the community. However, the government's policy in this regard would ultimately be underpinned by the collective moral responsibility of members of the community to save the lives of those threatened by the pandemic. However, as with the 9/11 example, and the fact that the government has access to a range of data sources about individuals it is important that this does not lead to normalization or more widespread use of metadata.

4 | CONCLUSION

This article has considered the technology responses mobilized by governments around the world to address the threat of the COVID-19 pandemic that had a significant impact on global health and economic activity in 2020. Smartphone metadata and Bluetooth applications have been used to assist in contact tracing and compliance with public health orders in a number of liberal democracies around the world. We have argued that there are implications for privacy and autonomy, particularly with respect to metadata (or GPS tracking) that monitors the location and movement of people, and to a lesser extent, Bluetooth applications, noting questions regarding the efficacy of the latter.

A conception of collective responsibility has been outlined that implies that there exists an individual moral responsibility to, for instance, download a Bluetooth application to reduce the threat of COVID-19 in the community, but that compliance should not necessarily be legally required or enforced. However, if voluntary compliance is not sufficient for the application to be effective, there is an argument for enforced compliance due to the significance of the COVID-19 threat for society and the reciprocal obligations generated by the web of interdependence. With regard to more invasive measures, such as the use of metadata in ways normally limited to the investigation of serious crimes, perhaps this should be restricted to specific cases where individuals known to have the disease would likely place others in the community at direct risk of contracting the disease. However, if metadata is accessed for this purpose, it is important that this does not lead to the normalization of this approach for public health or broader purposes.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

[37]The issue of the members of those occupations who are called upon to incur significant costs is an important one as is the question of the size of the costs relative to the seriousness and quantum of harm averted. However, addressing these issues is not directly relevant to our main concern in this paper.

ORCID

Seumas Miller https://orcid.org/0000-0002-4851-3177
Marcus Smith https://orcid.org/0000-0001-9810-979X

AUTHOR BIOGRAPHIES

Professor Seumas Miller holds research positions at Charles Sturt University, TU Delft and the University of Oxford. He is the Principal Investigator on a European Research Council Advanced Grant). His recent authored books include *Institutional corruption* (Cambridge University Press, 2017) and *Dual use science and technology, ethics and weapons of mass destruction* (Springer, 2018).

Marcus Smith is Senior Lecturer in Law at Charles Sturt University and Adjunct Professor of Law at the University of Canberra. He holds a PhD in law from the Australian National University. His recent books include *Technology law* (Cambridge University Press, 2021), *Biometrics, crime and security* (Routledge, 2018) and *DNA evidence in the Australian legal system* (LexisNexis, 2016).

How to cite this article: Miller S, Smith M. Ethics, public health and technology responses to COVID-19. *Bioethics*. 2021;35:364–371. https://doi.org/10.1111/bioe.12856