PART III

Legal and ethical considerations moving forward

11. Pandemic surveillance: ethics at the intersection of information, research, and health

Daniel Susser

This chapter provides a high-level overview of key ethical issues raised by the use of surveillance technologies, such as digital contact tracing, disease surveillance, and vaccine passports, to combat the COVID-19 pandemic. To some extent, these issues are entirely familiar. I argue that they raise old questions in new form and with new urgency, at the intersection of information ethics, research ethics, and public health. Whenever we deal with data-driven technologies, we have to ask how they fare in relation to important values like privacy, fairness, transparency, and accountability—values emphasized by information ethics scholars. Likewise, when such technologies put individuals at risk in order to drive scientific research and knowledge construction, we have to ask how they implicate values such as autonomy, beneficence and non-maleficence, and justice—values central to research ethics. And as researchers focusing on health information have long argued, when the data collected by these technologies pertain to individuals and public health, these ethical issues take on a special cast.

It is also true, however, that the pandemic has placed these questions in a new and revealing light. I highlight three insights from information ethics and research ethics that can help us navigate this difficult terrain. First, the value of privacy is instrumental, not absolute—there is nothing wrong with asking how to balance privacy against other important values. Second, privacy has both individual and social importance. Weighing privacy, on one hand, and public health, on the other, is not, therefore, a contest between individual and collective interests. Rather, it is an attempt to balance disparate public goods. Third, we ought to put these kinds of ethical decisions in the hands of third parties, rather than leaving them up to those who directly stand to benefit from them. In the case of pandemic surveillance technologies, this should mean more public, democratic oversight.

VALUES AT STAKE

Pandemic surveillance requires collecting, storing, analyzing, disseminating, and making decisions on the basis of huge amounts of information, raising critical questions that information and data ethicists have carefully studied. Several values tend to take center stage in these discussions: privacy, fairness, transparency, and accountability.

Questions about privacy ask how information about us flows. For example: Who collects information about us, by what means, and under which conditions? How to define privacy—and thus how to collect information in a manner that respects privacy—is the subject of significant controversy. Without trying to resolve these debates, here I draw attention to aspects of data collection that various approaches to privacy suggest are centrally important.

In US law and policy, information privacy is typically conceptualized as individual control over the flow of personal information (Westin, 2015). On this view, what matters most is that people are notified about data collection (digital or otherwise) and given the option to consent to or withhold consent from such collection at the initial point of capture (i.e., to "control" it) (Susser, 2019). The European Union's approach is more complicated. For present purposes, suffice it to say that it focuses on a more robust set of protections that aim not only to give individuals control over information about themselves (as the US approach does), but also to ensure that data collectors handle such information in ways that comport with European fundamental rights, and that third parties that buy and sell personal information are held to the same standards (Jones & Kaminski, 2021). A third approach to conceptualizing privacy is Helen Nissenbaum's theory of privacy as contextual integrity, which posits that norms governing how information ought to flow are intrinsically context-specific. On this view, the principal issue is whether data collectors gather and use information in ways that are contextually appropriate (Nissenbaum, 2010).

Thus, with respect to privacy, we might ask about pandemic surveillance technologies, such as contact tracing apps and vaccine passports, whether individuals are informed about the information that is being collected about them, about how it is used, and about the potential risks and benefits of its disclosure. Are they given the opportunity to choose whether to participate in these systems—to consent or withhold consent from data collection? Does data collection for the purposes of pandemic surveillance implicate European

fundamental rights? Does data collection respect contextual norms, or is data collected in one context being put to use in others?[1]

In contrast with worries about privacy, worries about fairness generally focus less on information collection and more on its analysis and use as the basis for important decisions, especially when decision-making is automated.[2] Scholars have long argued that computational systems can perpetuate bias, whether by impacting people unfairly, encoding discriminatory attitudes of their designers, or reflecting unjust social conditions in which they are designed and deployed (Friedman & Nissenbaum, 1996). These concerns are especially salient in relation to machine learning and other artificial intelligence systems—technologies that work by inferring decision-making logics, statistically, from data about past decisions, rather than by following rules articulated explicitly in advance. Such systems have been shown to be particularly susceptible to bias, because the datasets they learn from mirror historical patterns of injustice pervasive in society.[3]

The COVID-19 pandemic has affected different communities in different ways, often reflecting and deepening preexisting disparities (Wood, 2020). Without care and attention to questions about fairness, the technologies introduced to end the pandemic could make these disparities worse. Organizations developing and deploying such technologies ought to ask questions like: How is the data driving our decision-making collected? Are datasets equally representative of different social groups? What kinds of biases might reasonably be expected in the data, and how can they be adjusted for? How are decision-making outcomes distributed across social groups? Is information about group status—especially membership in protected classes, such as those related to race, gender, religion, and so on—affecting the decisions that automated systems reach?

Lastly, abstract concerns about privacy and fairness are of little practical value if violations and inequities cannot be detected and redressed. The values of transparency and accountability emphasize the importance of structures and practices that enable individuals, organizations, and communities to ensure other values are upheld. Transparency, as we've seen, is core to how privacy is operationalized in US law and policy—to respect individual privacy is, on

---

[1] For example, in Singapore, contact tracing data was appropriated by the police for law enforcement purposes (Illmer, 2021).

[2] This is not to say the two values are entirely independent. Privacy protections are often unequally distributed—with marginalized groups subjected to more surveillance than privileged groups—raising fairness concerns about privacy (see, e.g., Bridges, 2020).

[3] This issue has become the subject of a large and growing field of research (see, e.g., Mehrabi et al., 2021).

this approach, to make data collection and use transparent through privacy disclosures (i.e., "notice") and to seek individual consent in relation to it. But that is not the only relevant transparency requirement. Breach notification laws, for example, require data collectors to notify affected parties when information collected about them is exposed in a breach, and transparency requirements in the EU General Data Protection Regulation (GDPR) are designed to help people understand how automated decisions about them are reached (Bayamlıoğlu, 2018).

Worries about whether people subject to decision-making by automated systems can understand and contest decisions reached about them are becoming especially important as more decisions—both routine and significant—are delegated to computers. In the context of the COVID-19 pandemic, for example, we have seen some hospitals use automated decision-making systems to determine the order in which people were given access to vaccines (Harwell, 2020; Singer, 2021). To ensure that such systems and the organizations utilizing them are held to ethical standards, we should ask whether people know and understand that decisions about them are being made by automated systems, if the data and algorithms driving these systems are accessible to third-party auditors, and if their decision-making logics are explainable to the people they affect.

Pandemic surveillance implicates questions beyond those familiar to information ethics. Because one goal of pandemic surveillance is to advance scientific research on COVID-19, it also raises questions familiar to research ethics. These discussions generally focus on the values of autonomy, beneficence and non-maleficence, and justice.

Personal autonomy is the capacity for independent decision-making—the ability to choose for oneself, free from pressure, manipulation, or coercion (Roessler, 2021). It is a foundational value in liberal democratic societies, core to ideas of individual freedom and collective self-government. Research ethics, having developed partly in response to infamous cases of scientists experimenting on research subjects without their knowledge or against their will—such as Nazi medical experiments in World War II and the Tuskegee Syphilis Study, conducted for several decades in the middle of the 20th century—places significant emphasis on the right of individuals to choose freely, *autonomously*, to take part in scientific research. Usually, this right is operationalized through the mechanism of informed consent: before someone is implicated in scientific research, the person must be informed about it and given the opportunity to choose whether to participate (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979).

Where autonomy emphasizes free choice, the values of beneficence (i.e., "do good") and non-maleficence ("do no harm") point to the potential effects

of scientific research or experimentation on people's welfare. Will taking part in a scientific study make someone better or worse off? What are the risks and benefits associated with participation, both to research subjects and society more broadly? Beyond respecting the autonomy of research subjects by creating conditions under which they can freely choose whether to take part in research, research ethics expects that participants in scientific research will not be subjected to disproportionate risks, relative to the potential individual and societal benefits of the study (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979).

And as with fairness in discussions about information ethics, the focus on justice in research ethics emphasizes the need to ensure that the risks and benefits of scientific research are evenly distributed across social groups. Historically, marginalized groups have often been the first to be burdened by scientific research and the last to benefit from it, subjected to disproportionate risk relative to other groups and deprived of access to new treatments, techniques, and other fruits of successful research and experimentation. For example, in the Tuskegee Syphilis Study, treatment for the disease was withheld from most of the research subjects harmed in the experiment, even after therapies were widely available (Corbie-Smith, 1999). In designing research programs, it is therefore crucial to consider not only the rights and welfare of individual research subjects, but also the distribution of costs and benefits across society.

Developing pandemic surveillance technologies that advance scientific understanding of COVID-19 and help test treatments and strategies for combating it while respecting the core values of research ethics—autonomy, beneficence and non-maleficence, and justice—requires asking difficult questions and being prepared to make complex trade-offs. Will individuals subjected to these technologies be clearly informed about their implication in research, and will they be given the opportunity to make autonomous decisions about whether to participate? What are the specific costs and benefits of research, both to individuals and society? Do the benefits of particular research efforts outweigh potential harms? How are risks and benefits distributed across social groups? Are some groups exposed to disproportionate risk and others given access to disproportionate benefit? These are difficult questions, which cannot be resolved in the abstract; they must be raised in relation to each particular research effort and answered by considering its concrete design, manner of deployment, and expected impacts. As I discuss briefly in the next section, weighing such trade-offs is especially difficult in the context of a public health emergency like the COVID-19 pandemic. But we have no choice but to weigh them.

Finally, as if these ethical questions were not difficult enough, they are complicated further by the fact that they involve health information.

Obviously, health information can be highly sensitive, and the harms people suffer from its misuse are severe. Disclosing someone's health status can provoke powerful social stigma. Consider, for example, the stigma historically suffered by people who are HIV positive—especially gay men. Moreover, such disclosures can serve as the basis for harmful forms of discrimination in the provision of important goods, such as housing and employment. It is not difficult to imagine the kinds of stigma and discrimination that might result from careless stewardship of COVID-related health information, such as test results, vaccination status, or contact tracing data. Although other kinds of personal information, such as location information or internet browsing histories, can be very revealing and deserve significant protection, disclosure of health information threatens particularly acute harms.

In addition to being highly sensitive, health information raises complex ethics and policy challenges because its disclosure exposes not only the individuals it was collected from but also potentially their family members and other close associates. Genetic information provides the classic illustration of this problem: Given that our family members share a great deal in common with us genetically, revealing information about one person's genetic profile can be equally revealing of the person's parents, siblings, and children. Information about COVID diagnoses, vaccination status, and contact tracing creates similar dynamics: for example, knowledge that someone is COVID positive plausibly implicates people the person lives and works with. The nature of health information complicates the preceding discussion because, as we've seen, information ethics and research ethics often focus on empowering individuals. Yet it isn't clear that individuals should be empowered to decide whether to disclose information that might implicate their roommates or close kin.

LESSONS FOR AND FROM COVID-19

The ethical issues described in the previous section are complex and demanding. I want to highlight three insights from information ethics and research ethics that can help guide discussions about how to meet these challenges.

First, although privacy is often discussed in a way that suggests its value is absolute—that is, that it should never be traded off against other goods—most privacy scholars and advocates argue otherwise (see, e.g., Moore & Katell, 2016). Privacy is deeply important, for both individual and collective flourishing, but it is not good *in itself*. Rather, privacy is an instrumental value, something we pursue for what it affords us—the space for free thought and expression, reprieve from the judgmental gaze of others, the conditions for intimacy, and other essential goods (Warren & Brandeis, 1890; Fried, 1968,

pp. 478–480). When privacy and other values conflict, trade-offs have to be weighed.

COVID-19 furnishes a compelling case in point: many have argued that to bring the pandemic under control, we ought to give up privacy in the name of more accurate, granular contact tracing and disease surveillance. In other words, some argue that privacy is in tension with another centrally important (perhaps more important) value: public health. Others disagree. Privacy and public health are mutually compatible, they argue, because researchers have developed strategies for conducting contact tracing in a manner that is simultaneously accurate and privacy preserving (Apple & Google, 2021; Wacksman, 2021). Who has it right remains a subject of much debate. But if there really is a tension between privacy and public health, we need not commit to any particular resolution in advance. Even the most committed privacy proponents would likely concede that compelling people to disclose information about themselves—sacrificing some privacy—could be worth it for the sake of bringing the pandemic to an end, especially in conjunction with safeguards that ensure the information isn't used for other purposes.[4]

Second, there is a temptation to frame the ethical trade-offs described above as a conflict between an individual right (privacy) and a collective one (public health). Given the way that privacy is often theorized—especially in US law and policy—it is easy to understand why. However, this framing makes it very difficult, in practice, to resolve questions about how to balance these different kinds of goods. In pluralistic, liberal democratic societies there are deep disagreements about whether individual or collective interests ought to be given pride of place. Those on the libertarian side of the political spectrum argue that individual rights trump collective ones, while those on the social-democratic side argue the reverse. Thus, when framed as a contest between individual and collective pursuits, deciding whether to prioritize individual privacy or public health requires first resolving these more fundamental—perhaps intractable—tensions.

Yet privacy scholars have long argued that privacy is not *merely* good for individuals; it is also a social good (see, e.g., Cohen, 2012; Regan, 2000, pp. 212–217; Reidenberg, 1992; Nissenbaum, 2010). Which is to say, not

---

[4] Of course, privacy advocates can offer many other reasons against adopting invasive forms of surveillance and tracking, even under emergency conditions and in the name of public health. For example, technology studies scholars have long pointed out that surveillance infrastructures built for one purpose tend to be put to other uses—so-called "surveillance creep" (Marx, 1988). Indeed, we have already seen this in the context of pandemic technologies, in the Singapore case mentioned above. The point here is that privacy is something that *can* be balanced against other important values. Whether it ought to be has to be determined case by case.

only are we individually worse off without privacy, but society as a whole is worse off without it. Absent privacy, societies are more conformist and less open. They do not benefit from the new, challenging ideas people are able to advance when they have the privacy to entertain and develop them. And such societies can easily give way to authoritarian forms of power, if individuals are not allowed to live significant parts of their lives free from unwanted surveillance. Framing the problem this way helps us see that we are not dealing with a problem of reconciling two different kinds of interests—individual privacy versus public health. Rather, it's a question of balancing two public goods: How should we trade off the social benefits of privacy against the social benefits of public health? In this way, emphasizing the social value of privacy can help us avoid unproductive debates about the relative importance of individual and collective goods.

Third and finally, research ethics reminds us that when arbitrating between competing values, it is often important to solicit the perspective of a neutral third party, a person or an institution that does not stand to benefit directly from the decision. In research ethics, that third party is usually an institutional review board, or IRB. We do not ask the scientists proposing sensitive research to determine for themselves whether its potential benefits outweigh potential costs—to experimental subjects or society at large. We task a panel of peer scientists, ethicists, and members of the public to independently make that determination.

In the case of pandemic surveillance technologies, we may want to create similar decision-making structures. Rather than expecting individual companies, health departments, and other institutions to make these ethical decisions on their own, we should place them in the hands of third parties—for example, independent ethics boards or regulatory agencies. Better yet, we should demand democratic oversight. This could take many different forms: opportunities for public comment and debate, citizen juries or so-called "minipublics," or formal votes in local or national legislatures (Greitens, 2020, pp. 182–185; Fung, 2007). Whatever the mechanism, we could decide collectively how to navigate the difficult ethical challenges raised by these difficult circumstances.

REFERENCES

Apple & Google. (2021, April). "Exposure Notification Privacy-preserving Analytics (ENPA)" [White Paper]. https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ENPA_White_Paper.pdf

Bayamlıoğlu, E. (2018). "Transparency of automated decisions in the GDPR: An attempt for systemisation." http://dx.doi.org/10.2139/ssrn.3097653

Bridges, K. M. (2020). *The Poverty of Privacy Rights*. Stanford University Press.

Cohen, J. E. (2012). "What privacy is for." *Harvard Law Review*, 126, 1904–1933.

Corbie-Smith, G. (1999). "The continuing legacy of the Tuskegee Syphilis Study: Considerations for clinical investigations." *American Journal of the Medical Sciences*, 317(1), 5–8. https://doi.org/10.1016/S0002-9629(15)40464-1

Fried, C. (1968). "Privacy." *Yale Law Review*, 77(3), 475–493. https://doi.org/10.2307/794941

Friedman, B., & Nissenbaum, H. (1996). "Bias in computer systems." *ACM Transactions on Information Systems*, 14(3), 330–347.

Fung, A. (2007). "Minipublics: Deliberative designs and their consequences." In S. Rosenberg (ed.), *Deliberation, Participation and Democracy: Can the People Govern?* (pp. 159–183). Palgrave Macmillan. https://link.springer.com/chapter/10.1057/9780230591080_8

Greitens, S. C. (2020). "Surveillance, security, and liberal democracy in the post-COVID world." *International Organization*, 74(S1), E169–E190.

Harwell, D. (2020, December 23). "Algorithms are deciding who gets the first vaccines. Should we trust them?" *Washington Post*. www.washingtonpost.com/technology/2020/12/23/covid-vaccine-algorithm-failure/

Illmer, A. (2021, July 5). "Singapore reveals Covid privacy data available to police." BBC. www.bbc.com/news/world-asia-55541001

Jones, M. L., & Kaminski, M. E. (2021). "An American's guide to the GDPR." *Denver Law Review*, 98, 93–128.

Marx, G. (1988). *Undercover: Police Surveillance in America*. University of California Press.

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). "A survey on bias and fairness in machine learning." *ACM Computing Surveys*, 54(6), 1–35. https://doi.org/10.1145/3457607

Moore, A., & Katell, M. (2016). "Introduction." In A. Moore (ed.), *Privacy, Security, and Accountability: Ethics, Law, and Policy*. Rowman and Littlefield.

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). "The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research." US Department of Health and Human Services.

Nissenbaum, H. F. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Regan, P. M. (2000). *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press. www.jstor.org/stable/10.5149/9780807864050_regan

Reidenberg, J. R. (1992). "Privacy in the information economy: Fortress or frontier for individual rights." *Federal Communications Law Journal*, 44(2), 195–244.

Roessler, B. (2021). *Autonomy: An Essay on the Life Well Lived*. Polity Press.

Singer, N. (2021, February 7). "Where do vaccine doses go, and who gets them? The algorithms decide." *New York Times*. www.nytimes.com/2021/02/07/technology/vaccine-algorithms.html

Susser, D. (2019). "Notice after notice-and-consent: Why privacy disclosures are valuable even if consent frameworks aren't." *Journal of Information Policy*, 9, 148–173. https://doi.org/10.5325/jinfopoli.9.2019.0148

Wacksman, J. (2021). "Digitalization of contact tracing: Balancing data privacy with public health benefit." *Ethics and Information Technology*, 1–7.

Warren, S., & Brandeis, L. (1890). "The right to privacy." *Harvard Law Review*, 4(5), 193–220. https://doi.org/10.2307/1321160

Westin, A. (2015). *Privacy and Freedom*. IG Publishing.

Wood, D. (2020, September 23). "As pandemic deaths add up, racial disparities persist—and in some cases worsen." NPR. www.npr.org/sections/health-shots/2020/09/23/914427907/as-pandemic-deaths-add-up-racial-disparities-persist-and-in-some-cases-worsen