AI Surveillance during Pandemics: *Ethical Implementation Imperatives*

by Carmel Shachar, Sara Gerke, and Eli Y. Adashi

Artificial intelligence can be used to help track the spread of Covid-19, diagnose individual cases, and help provide care. The AI startup BlueDot, based in Toronto, detected the outbreak in Wuhan before the general Chinese population was apprised by way of official announcements. The Chinese technology giant Alibaba developed an AI system that can quickly detect coronavirus in CT scans with 96 percent accuracy. Recent scholarship has suggested that SARS-CoV-2 spreads too rapidly for manual contact tracing to be effective but that an automated contact-tracing surveillance program could control the spread of Covid-19 to the point where mass quarantines would no longer be needed.[1] Jared C. Kushner, President Trump's senior advisor, is spearheading a collaboration between the Department of Health and Human Services and technology firms to establish a public health surveillance system, which some members of Congress have called a threat to privacy.[2] The health needs created by the pandemic put significant pressure on physicians, hospital leaders, public health officials, and other care providers to collaborate with developers to create new AI applications to combat Covid-19.

These promising applications, however, raise several legal and ethical concerns, ranging from privacy to discrimination to access to care. Health care systems seeking to manage the pandemic through use of AI must be sensitive to these risks. Some violations of patient rights cannot be undone after an outbreak. Luckily, there are several frameworks that can help guide stakeholders—especially physicians but also AI developers and public health officials—as they navigate these treacherous shoals. These frameworks include international, national, and state laws as well as guidance from bioethics organizations, such as the Nuffield Council on Bioethics and The Hastings Center, and public health organizations, such as the World Health Organization (WHO), and the Centers for Disease Control and Prevention (CDC). Although not explicitly designed for AI surveillance during a pandemic, these frameworks can be adapted to help address concerns about privacy, human rights, and due process and equality.

Privacy

While AI-based technologies have much to offer in combating Covid-19, they also pose real risks to privacy. China used AI to perform contact tracing and to manage priority populations, thereby contributing to the country's aggressive and successful response to Covid-19. Israel likewise announced that it will make use of digital surveillance in the containment of Covid-19. Singapore developed TraceTogether, an app that uses Bluetooth data to perform rapid contact tracing. This app has inspired similar efforts in other countries, such as Germany. In the world of machine learning and AI, it becomes crucial to apply privacy laws to adequately protect health data of individuals collected online or through apps and wearables. The European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are examples of statutes and regulations that address privacy concerns. Moreover, the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule offers some, but not complete, protection for certain individually identifiable health information.

In a public health emergency, public health authorities and private actors must not only comply with the applicable regulatory frameworks, including the use of anonymized or deidentified data whenever possible, but also consider broader privacy questions. This is vital since privacy violations are unlikely to be remedied in the aftermath of a pandemic. HIPAA contains an exception to data disclosed for public health activities.[3] However, it is unlikely that this exception would be extended to a private company seeking to leverage AI to redress a pandemic. At the same time, much of the data generated by AI surveillance programs will not be covered under HIPAA in the first place and may lack protection entirely. For example, cell phone geolocation data do not fall under HIPAA but are sensitive data that now reveal information about one's Covid-19 risk. Information collected outside the clinic or hospital, such as via Covid-19 screening and testing by Google's sister company Verily, are also not protected by HIPAA. But Verily needs to comply at least to the CCPA when offering services to California residents. The CCPA gives several rights to California residents, including the right to opt out of sales of their personal information to third parties.[4] Individuals depend on the laws of their state for the extent to which their privacy is protect-

ed. When it comes to AI surveillance for the purpose of combating Covid-19, HIPAA's scope is too limited.

The processing of special categories of personal data, such as health data, is usually prohibited under the European Union's GDPR, but the regulation contains some exceptions. In particular, Article 9(2)(i) explicitly states that the general processing ban of special categories of personal data shall not apply where "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health . . . on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."[5] Thus, the processing of data concerning health is likely allowed during Covid-19, without the need for the explicit consent of the individual concerned.[6] But for mobile location data, additional rules apply. The European Data Protection Board recently clarified that "the public authorities should first aim for the processing of location data in an anonymous way."[7] When this is not possible, Article 15 of the ePrivacy Directive allows the EU member states to introduce emergency legislation. However, such legislation must constitute "a necessary, appropriate and proportionate measure within a democratic society."[8] In addition, the member state must "put in place adequate safeguards, such as granting individuals the right to judicial remedy."[9]

Regulators and stakeholders should look to ethical guidelines to craft data privacy controls for AI surveillance programs, especially when addressing gaps in existing privacy regulatory regimens. The "Guide to the Ethics of Surveillance and Quarantine for Novel Coronavirus" ("Guide to the Ethics of Surveillance"), issued by the Nuffield Council on Bioethics, acknowledges that "to assess and predict trends in infectious disease it is acceptable for anonymised data to be collected and used without consent, as long as any invasion of privacy is reduced as far as possible. It may be ethically justified to collect nonanonymised data about individuals without consent if this means that significant harm to others will be avoided."[10] To guide the distinction between uses of anonymized and nonanonymized data, AI surveillance governance could also draw from HIPAA's strong distinction between deidentified and protected health information (that is, individually identifiable health information). The sharing of individually identifiable health information by HIPAA-covered entities (which includes most health care providers) with private companies capable of facilitating the creation of surveillance networks may be justified when the companies are considered "business associates" under HIPAA. In contrast, deidentified data can usually be freely used, for example, for commercial purposes.

AI surveillance regulations emphasize that data should be kept deidentified or anonymized whenever possible so long as the ultimate goal of protecting public health is achieved, even if the use of anonymized data may come with trade-offs in efficiency. When nonanonymized data is needed, extra safeguards should be put in place to protect privacy. Any technology company looking to build a public health surveillance program with nonanonymized data should be required to sign a memorandum of understanding with its governmental partners, a document similar to the business-associate agreements mandated under HIPAA. These memorandums would contain data privacy and security safeguards. For example, they would articulate the precautions that must be taken to avoid misuse of nonanonymized data, including limiting access to this data set to a select number of employees and officials who also need to enter into a confidentiality agreement before receiving access to the data. Moreover, these memorandums would provide a "right to be forgotten" mechanism akin to those provided in the GDPR and CCPA. This right would ensure that all Americans with strong objections to the programs could request the erasure of their data as soon as the processing of nonanonymized data is no longer necessary for public health reasons. Additionally, the technology company and its governmental partners should provide a public notice and justification for why the use of nonanonymized data is "necessary, appropriate and proportionate" to allow consumer advocates the opportunity to contest the use. Finally, any ethical regulation of a broad AI surveillance program should ban commercial use of nonanonymized public health surveillance data and prohibit the use of this data by the criminal justice system. Deidentified data generated by this program, however, may be used to incentivize commercial partners or for broader public policy purposes as long as proper safeguards are in place to minimize the risk of reidentification.[11] These safeguards, including the memorandums, public notice and justification, and prohibited ancillary uses, ensure that individuals' privacy will be protected as best as possible.

Human Rights

Apart from privacy laws, several other international and national laws, regulations, and guidance documents can help physicians and other stakeholders evaluate and ethically implement AI and related surveillance technologies for health purposes. Mass quarantines enforced by technology, while effective, raise human rights concerns. For example, mobile phone apps can track individuals' movements, thereby allowing governments to prevent people deemed to be infected or at-risk from traveling. Societies must consider what is being traded in return for such strong social controls. Will societies accede to similarly effectuated surveillance of people living with diseases and disorders unrelated to SARS-CoV-2 or the cause of a future epidemic?

Existing frameworks address these concerns. Article 43 of the WHO's *International Health Regulations* requires countries to limit those public health measures that impose restrictions on international traffic to ones that are supported by science, respect human rights, and are proportional to the risks.[12] The "Guide to the Ethics of Surveillance" also allows for liberty-infringing mea-

sures but only "if the risk of harm to others can be significantly reduced."[13] In a string of cases, mostly involving persons with mental illness, the Supreme Court of the United States articulated three key requirements for civil commitment: an individualized risk assessment, the least restrictive means necessary, and due process rights.[14] This case law is also echoed in the CDC's "Ethical Guidelines in Pandemic Influenza," which calls for the suspension of individual liberties only when "the least restrictive practices that will allow the common good to be protected" are chosen.[15] The U.S. framework has parallels in the "Guide to the Ethics of Surveillance," which urges states to use the least coercive means necessary to implement public health surveillance programs—coupled with transparent and accountable decision-making processes where consent is not possible.[16]

AI surveillance products should be developed with the goal of pursuing the least coercive means and be respectful of human rights whenever possible. Drawing on the framework provided by the WHO's Article 43, policy-makers should require AI surveillance programs for use during the current pandemic to be continually redesigned to reflect evolving understanding of Covid-19. For example, right now, it is unclear exactly how close individuals need to be and for what duration for SARS-CoV-2 to spread from person to person. An AI surveillance system might currently include two joggers who briefly run side by side as potential contacts. But if we learn that SARS-CoV-2 cannot infect through this type of exposure, we would want to modify that system to remove those incidents. AI surveillance implementers should be transparent about the underlying assumptions their models make about the spread of Covid-19.

The human rights frameworks also call for careful consideration of how the outcomes of AI surveillance will affect individuals. Is it merely that one's contacts would be notified that their risk of Covid-19 is heightened? Or would a person be required to quarantine? If you break quarantine, will the AI surveillance system notify the relevant authorities, and will there be liability for your actions? An AI surveillance program that merely notifies those at risk is less fraught than a program that results in criminal charges for leaving one's home once one is flagged as at risk. The least-coercive-means theme that runs through virtually all the relevant frameworks suggests that one should aim for the least-intrusive outcomes of surveillance. Only if notification proves to be ineffective at controlling the spread of the disease may harsher outcomes be justified. In regard to outcomes beyond notification, mandatory measures should be the last resort. Stay-at-home practices, including those targeting high-risk groups such as the elderly or people with preexisting conditions, should be voluntary whenever possible.

Ensuring Due Process and Equality

Questions may well arise about both due process and racial discrimination when certain groups are targeted as the "vectors" of a disease. In *Jew Ho v. Williamson*, a federal court overturned a racially motivated mass quarantine of San Francisco's Chinatown as a violation of the equal protection clause of the Fourteenth Amendment.[17] The WHO's *Guidance for Managing Ethical Issues in Infectious Disease Outbreaks* also calls for equitable application of any restrictions on freedom of movement, with such restrictions based solely on the risk posed to others and without a disproportionate burden on vulnerable populations.[18] Similarly, The Hastings Center's "Ethical Framework for Health Care Institutions Responding to Novel Coronavirus SARS-CoV-2 (COVID-19): Guidelines for Institutional Ethics Services Responding to COVID-19" reminds us that public health leaders have a duty to protect vulnerable populations.[19]

To fulfill ethical duties to the uniquely vulnerable and avoid discrimination in the use of AI, stakeholders must be transparent about which communities and individuals are being monitored. Implementers of AI surveillance programs should keep in mind that lower-income individuals, many of whom cannot work from home and do not have the financial reserves to weather long periods of unemployment, may feel the brunt of an AI surveillance system more strongly than higher-income individuals may. Borrowing from the disability rights movement, "Nothing about us, without us" should be a central tenet of designing AI surveillance systems. Community leaders should be involved so that they can flag when their members are being unfairly affected.

Due process can help ensure the ethical implementation of health AI. New York City regulations,[20] for example, allow for the isolation of individuals with tuberculosis only with certain protections, such as a periodic judicial review. Implementation of any AI-based surveillance products should incorporate similar safeguards to avoid due-process violations. Implementers of AI surveillance programs should be transparent about the programs' reach. For instance, Covid-19 infection rates are not consistent across the United States. Articulating guidelines for when AI surveillance will be implemented, perhaps in response to a spike in infection rates, and when these programs will be discontinued would provide substantive due process. Requiring periodic judicial review of AI surveillance programs would also ensure that the programs continue no longer than necessary. Any AI surveillance program should include a mechanism for individuals to contest any resultant quarantine. Individuals flagged by the surveillance program for quarantine should also be entitled to social or financial support, from either their employers or the state, to meet the terms of their quarantine.

The Nature of the Actors Involved

Of course, human rights, due process, and judicial review are usually applied to state actions and not the actions of private actors. In some countries, AI surveillance will be implemented by governments, perhaps in partnership with technology companies. For these systems, the relevant obligations and responsibilities are partially

specified. American governmental actors, for instance, must abide by Fourth Amendment jurisprudence, which protects people from unlawful searches and seizures by the government, especially in the privacy of their own home. It will be more complicated when AI surveillance is implemented by private actors or volunteers. For instance, people may voluntarily provide information to a tracking system that will, in turn, supply an analysis or information to current or prospective employers. Or hospital systems may ask individuals to share information from Fitbits and other wearable sensors so that they can decide where best to allocate resources or deploy workers. Private actors should consider frameworks that already exist and also import concepts of due process.

For employers, significant guidance is available on the use of medical information in the workplace. The U.S. Equal Employment Opportunity Commission, for example, released the document "Pandemic Preparedness in the Workplace and the Americans with Disabilities Act."[21] This guidance allows employers to ask medical questions of their current employees only to determine if the employee's ability to perform essential job functions will be impaired by the medical condition or to determine if the employee poses a direct threat to the workplace or to others. An AI surveillance system should limit employer access such that it is triggered only if essential job functions are impaired or if a direct threat exists.

Additionally, even if private actors do not have the same obligations and responsibilities as governmental actors, nothing prevents private actors from drawing on these frameworks and concepts to ensure "best ethical hygiene." Considering the broad reach of AI surveillance, developers and users of these systems should consider the building blocks of due process, such as the ability to appeal a decision, and incorporate them into their AI surveillance systems. While the least-restrictive means necessary is a concept usually applied to state action, especially in the case of constitutional and human rights, it should also be a guiding star for private actors who are developing AI surveillance. What is the least burdensome way to achieve the surveillance goals? How can the impact on individuals be minimized? Considering the potential of even voluntary AI surveillance systems to undermine privacy and freedom of movement, AI developers should strive for the highest ethical standards possible in designing these programs.

Although AI can be deployed to better deal with outbreaks such as Covid-19, health care providers and health technology companies must always, even in times of crisis, comply with existing regulations, such as applicable data privacy provisions. Health AI products should be designed and implemented with ethical frameworks in mind, incorporate the least coercive means, and assure due process. Although the balance between individual rights and public interest may shift during times of crisis, that does not mean that existing frameworks should be disregarded.

Disclosure

Eli Adashi serves as the cochair of the Safety Advisory Board of Ohana Biosciences, Inc.

Acknowledgment

This work was supported by a grant from the Collaborative Research Program for Biomedical Innovation Law, a scientifically independent collaborative research program supported by a Novo Nordisk Foundation grant (NNF17SA0027784).

1. L. Ferretti et al., "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing," *Science* 368 (2020): doi:10.1126/science.abb6936.

2. M. Warner, R. Blumenthal, and A. Eshoo, "Letter to Jared Kushner," April 10, 2020, https://www.warner.senate.gov/public/_cache/files/b/7/b7f6f957-80ed-4517-8290-84ba40e14396/3936C6E0ECF295C1EE5447F52486AA33.kushner-health-privacy-letter-clean.pdf.

3. 45 C.F.R. 164.512(b).

4. Cal. Civ. Code § 1798.120.

5. Office of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the processing of personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union* (2016).

6. "Statement by the EDPB Chair on the Processing of Personal Data in the Context of the COVID-19 Outbreak," European Data Protection Board, March 16, 2020, https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en.

7. Ibid.

8. Ibid.

9. Ibid.

10. Nuffield Council on Bioethics, "Guide to the Ethics of Surveillance and Quarantine for Novel Coronavirus," February 10, 2020, https://www.nuffieldbioethics.org/assets/pdfs/Guide-to-the-ethics-of-surveillance-and-quarantine-for-novel-coronavirus.pdf.

11. S. Gerke, S. Yeung, and I. G. Cohen, "Ethical and Legal Aspects of Ambient Intelligence in Hospitals," *Journal of the American Medical Association* 323 (2020): 601-2.

12. World Health Organization, *International Health Regulations (2005)*, 2nd ed. (Geneva: WHO, 2008), at http://www.who.int/ihr/publications/9789241596664/en/.

13. Nuffield Council on Bioethics, "Guide to the Ethics of Surveillance."

14. Addington v. Texas, 441 U.S. 418 (1979); O'Connor v. Donaldson, 422 U.S. 563 (1975); Jackson v. Indiana, 406 U.S. 715 (1972).

15. "Ethical Guidelines in Pandemic Influenza," Centers for Disease Control and Prevention, February 15, 2007, https://www.cdc.gov/od/science/integrity/phethics/docs/panflu_ethic_guidelines.pdf, p. 5.

16. Nuffield Council on Bioethics, "Guide to the Ethics of Surveillance."

17. Jew Ho v. Williamson 103 F.10 (C.C.N.D. Cal., 1900).

18. World Health Organization, *Guidance for Managing Ethical Issues in Infectious Disease Outbreaks* (Geneva, Switzerland: WHO, 2016), https://apps.who.int/iris/bitstream/handle/10665/250580/9789241549837-eng.pdf;jsessionid=01365A87B706B2BA54612A6F8D08DBCC?sequence=1.

19. N. Berlinger et al., "Ethical Framework for Health Care Institutions Responding to Novel Coronavirus SARS-CoV-2 (COVID-19): Guidelines for Institutional Ethics Services Responding to COVID-19," The Hastings Center, March 16, 2020, https://www.thehastingscenter.org/wp-content/uploads/HastingsCenterCovidFramework2020.pdf.

20. New York, N.Y., tit. 24, Health Code § 11.21.

21. "Pandemic Preparedness in the Workplace and the Americans with Disability Act," U.S. Equal Employment Opportunity Commission, 2009, updated March 21, 2020, https://www.eeoc.gov/facts/pandemic_flu.html.

DOI: 10.1002/hast.1125