Ethics and governance for digital disease surveillance

The question is not whether to use new data sources but how

By **Michelle M. Mello**[1,2] *and* **C. Jason Wang**[1,3]

Digital epidemiology—the use of data generated outside the public health system for disease surveillance—has been in use for more than a quarter century [see supplementary materials (SM)]. But several countries have taken digital epidemiology to the next level in responding to COVID-19. Focusing on core public health functions of case detection, contact tracing, and isolation and quarantine, we explore ethical concerns raised by digital technologies and new data sources in public health surveillance during epidemics. For example, some have voiced concern that trust and participation in such approaches may be unevenly distributed across society; others have raised privacy concerns. Yet counterbalancing such concerns is the argument that "sometimes it is unethical *not* to use available data" (*1*); some trade-offs may be not only ethically justifiable but ethically obligatory. The question is not whether to use new data sources—such as cellphones, wearables, video surveillance, social media, internet searches and news, and crowd-sourced symptom self-reports—but how.

INNOVATIONS AGAINST COVID-19

Some efforts involve escalations of existing techniques of digital epidemiology—for example, using cellphone signals and social media data to map the spread of the virus—whereas other, more innovative initiatives focus on implementing public health measures such as isolation and quarantine.

Disease modeling and forecasting using machine learning and artificial intelligence

There is growing potential to use machine learning and big data to forecast disease spread and prioritize people for testing or limitations on movement. One controversial application during the COVID-19 outbreak has been the Chinese government's requirement that citizens in more than 200 cities install an Alipay app on their smartphones that assigns a risk code to each person indicating the extent to which they are permitted to move around the community (see SM). The coding algorithm reportedly incorporates information on time spent at risky locations and frequency of contact with other people. Public dissatisfaction with the app arose from lack of transparency about the reasons people were classified into particular groups and mismatch with individuals' own beliefs about their risk level. Yet algorithmic classification and prioritization of individuals or localities may offer an alternative to haphazard rollout of social distancing orders and COVID-19 testing.

Leveraging and linking large datasets for case identification

Governments have massive troves of citizens' personal data at their disposal that can be used to identify persons at increased risk of infection and prioritize them for investigation by health officials. The Taiwanese government linked immigration and customs data on travelers (in batch files, after deleting irrelevant travel history) to National Health Insurance data on hospital and clinic visits to identify individuals whose symptoms could be due to contracting the novel coronavirus during travel to an affected area (*2*). That information was shared with health care providers so that they could use it to make decisions during patient visits, such as asking for additional history of present illness and ordering a COVID-19 test.

Risk-based border security

Taiwan developed an interesting alternative to blanket travel restrictions: individualized risk assessment. Travelers scan a QR code using their smartphone, which leads to an online travel declaration form that asks for travel history and flight information, symptoms of fever or respiratory infection, and contact information in Taiwan. On the basis of their health and travel information, travelers are either sent a pass by text, asked to do home quarantine for 14 days, or instructed to self-isolate at home for 14 days (*2*).

Electronic monitoring of quarantined and isolated individuals

New Zealand, Thailand, and Taiwan use cellphone location data to monitor movement of persons subject to quarantine or isolation orders. In Taiwan, for example, violators can receive heavy fines or be ordered into facilities, but the government first messages individuals to instruct them to return home and asks local police to check on them (*2*). China, Poland, and Russia have gone further, using facial recognition software to monitor compliance with orders (see SM). Such measures, although intrusive, help reduce the need for labor-intensive, in-person monitoring. De-identified location data from cellphones and social media apps can also be used to monitor population-level adherence to social distancing orders (see SM).

Digital technologies are also useful for supporting confined individuals. Remote monitoring through smartphones improves

Whether to implement, how to implement

What is the alternative?
Whether to adopt a digital surveillance measure should be evaluated by referencing the counterfactual. What would be used instead of the technology, and is that more or less desirable?

Least burdensome alternative
For its use to be justified, a digital technology should be judged the least burdensome alternative that would accomplish the public health objective.

Public oversight
Oversight must include members of the public; focus on particular uses of the data, not just data transfers; and promote trustworthy, transparent, and convincing justifications for the decisions taken.

Correcting mistakes
Processes through which potential errors can be challenged in the courts may be modified, involving longer waits, less robust hearings, and reduced access to counsel. Proving mistakes can be difficult where a decision has been driven by an algorithm whose logic may not be transparent.

Inequities and bias
Inequities persist in people's access to the internet and cellphones. Even among those having access, disparities exist in who uses these technologies. These disparities risk creating bias in new data sets.

[1]Center for Health Policy/Primary Care and Outcomes Research, Department of Medicine, Stanford University School of Medicine, Stanford, CA, USA. [2]Stanford Law School, Stanford, CA, USA. [3]Department of Pediatrics and Center for Policy, Outcomes and Prevention, Stanford University School of Medicine, Stanford, CA, USA.
Email: mmello@law.stanford.edu

the prospects for isolating and quarantining people at home rather than in facilities. People's temperatures can be transmitted by wearables, digital thermometers, or video, and health workers can regularly check on people's needs without exposing themselves to the risk of transmission. Communities, too, can mobilize to assist those confined at home, as is occurring in the United States through the neighborhood social networking app NextDoor.

Enhanced contact tracing

Serious doubts have been raised about whether traditional methods of contact tracing alone can arrest the COVID-19 epidemic. Adding algorithmic contact tracing through a cellphone app or operating system is proposed to reduce transmission of the virus through instantaneous notification of contacts (see SM) (*3*). A real-world experiment with such an approach is under way in Singapore, where in March 2020 the government requested that citizens install a government-developed smartphone app called TraceTogether. The app uses Bluetooth technology to exchange identifier numbers with the phones of other TraceTogether users within 6 feet of the user, sharing data with the government only if the user becomes subject to contact tracing because of a COVID-19 diagnosis (see SM). As of late April 2020, similar apps have been rolled out in nearly 30 countries, and a high-profile effort by Google and Apple to develop standards is under way (*4*).

The Israeli government has gone farther than Singapore, making use of infected persons' cellphone location data on an involuntary basis. Its approach sends texts to persons who come into contact with known COVID-19 cases to inform them that they must immediately quarantine themselves for 14 days (*5*). South Korea, too, has opted to use geolocation data without seeking consent. It publicly posts information on where infected persons traveled in the days before their diagnosis based on cellphone location data, credit card records, and surveillance video (*5*). No names are included, but individuals' age, nationality, and sex are. Taiwan used itineraries of passengers who disembarked the Diamond Princess cruise ship to send text alerts to people residing in areas the passengers visited, asking them to self-monitor and notify officials of any symptoms. The recipient list was compiled by using mobile phone base station positioning.

ETHICAL ISSUES RAISED

Ethical issues raised by digital epidemiology center on a core tension: these new uses of people's data can involve both personal and social harms, but so does failing to harness the enormous power of data to arrest epidemics.

Respecting privacy

Many epidemiologic uses of new data sources do not implicate informational privacy to a greater extent than current commercial and research practices—although some people may feel greater disquiet about governments using their data than they do companies or academics. Other uses involve larger potential intrusions on privacy. Using cellphone location and text data, in particular, goes beyond what citizens of democratic nations are accustomed to. Everyday uses of public and private data are typically not conducted with personal identifiers attached. Moreover, except for use by law enforcement, data are not ordinarily used for purposes of tracking down and imposing consequences on the subjects of the data. Contact tracing of the kind being carried out in Israel, by contrast, involves immediately imposing public health orders on those traced.

Respecting autonomy

Respect for individuals' autonomy generally requires asking them for permission to access their personal information and use it in particular ways. Informed consent is a bedrock principle of research ethics and medical care and is expressed—albeit weakly—in Terms and Conditions agreements for use of websites and apps, which ask users to agree to the company's planned uses of their data. The consent issue has particular salience for contact tracing through cellphone records because at least three alternative regimes—opt in, opt out, and mandatory—are possible, and different countries have made different choices.

Equity concerns

Use of new data sources can improve representation of some populations in epidemiologic analysis, including people who are underrepresented in data from laboratories and health care providers because they cannot or do not access care. Nevertheless, inequities persist across the globe in people's access to the internet and cellphones. Even in areas with access, disparities exist in who uses these technologies (see SM). These disparities risk creating bias in new data sets.

Minimizing the risk of error

The risk that governments will make errors in identifying areas and individuals at high risk of disease infection is heightened when using new data because of three factors: scope, speed, and sources. First, the use of large datasets means that a much greater number of people are under review than would ordinarily be the case; errors in even a small percentage of cases translate into large numbers of people affected. Second, the pressure to develop and roll out apps and algorithms quickly during an emergency may mean compromises on testing and validation. But erroneously flagging individuals or areas can involve serious social and economic burdens, such as stay-at-home orders and business closures. Mistakes also undermine trust and waste limited public health resources (*6*). Third, the sources of information in some new datasets will be less reliable than traditional disease reporters. Particularly given the spread of misinformation about disease outbreaks through social media, the need to validate data derived from internet news, search data, and social media posts is acute. Self-reports of perceived symptoms, too, may be inaccurate or incomplete and are not easy to corroborate (see SM).

Correcting mistakes can pose special challenges during public health emergencies, underscoring the importance of taking steps up front to minimize the risk of error. Ordinary processes though which citizens and businesses can challenge public health orders in the courts may be modified, involving longer waits, less robust hearings, and reduced access to counsel. Proving mistakes can also be difficult when a decision has been driven by an algorithm because algorithmic logic is often not transparent.

Accountability

A key question is how to ensure that companies and governments conducting and using epidemiologic analyses of new data sources are accountable for what they do. Democratic processes ordinarily help ensure that policymaking is reasonably transparent, the public has opportunities for input, and irresponsible officials can be removed. But many initiatives during COVID-19 have been undertaken by countries without strong democratic traditions and free-speech protections. Even in the United States, technological solutions are being pursued by small groups of officials and tech company leaders working outside ordinary channels and public view. The need to make decisions quickly may justify such processes but increases concerns about responsible practices.

The potential for misappropriation of data collected and methods developed for disease surveillance looms large. After all, the same approaches that can be used for case identification and contact tracing can be used to identify and track a government's political opponents (*5*). Such fears undercut trust in what public health officials are trying to do, and without public trust and participation, many key strategies for fighting infectious disease cannot succeed.

POLICY RECOMMENDATIONS

Two principles should serve as lodestars when considering the ethics of digital surveil-

lance during pandemics. First, the wisdom of adopting a digital surveillance measure should be evaluated not in the abstract but by reference to the counterfactual. What would be used instead of the technology, and is that more or less desirable? The counterfactual for COVID-19 involves mass shelter-at-home and business closure orders, which impose serious liberty and economic deprivations and are, in most areas, completely nonconsensual. Digital surveillance offers the prospect of expediting the lifting of such orders and minimizing their use in future outbreaks (*3*). It may have particular value for vulnerable groups such as the elderly and persons with chronic illness who may otherwise remain confined after others are released.

The second principle is that for its use to be justified, a digital technology should be judged the least burdensome alternative that would accomplish the public health objective (*7, 8*). This principle has long driven thinking in public health ethics and law. For disease outbreaks, what constitutes the least restrictive alternative depends on the available public health resources, evidence concerning what behaviors people will engage in without coercive public health orders, features of the pathogen's transmissibility, and the stage of the epidemic. Even if such a weighing points toward the imposition of digital surveillance, the least restrictive alternative principle can help minimize privacy intrusions—for example, through data minimization (identifying the narrowest possible set of data elements, especially identifiable ones, and the minimum duration and scope of use required to achieve the objective) (*8*). We consider applications of these two principles to particular technologies with value in combating the novel coronavirus and similar pathogens.

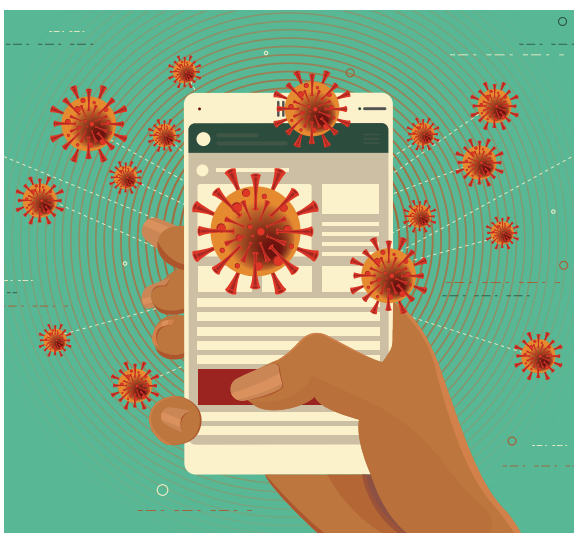

ILLUSTRATION: ADAPTED FROM THINKNEO/ISTOCK.COM

Using algorithms in disease modeling and risk classifications

The use of artificial intelligence techniques for disease forecasting raises minimal ethical concerns if it uses individually deidentified data. But using personally identifiable information in algorithms that assign risk scores or categories to individuals, such as in the case of the Alipay app, must be considered more seriously because of the social consequences attached to these determinations. Here, the main concerns are the usual ones about algorithmic bias and error, and solutions offered for such problems in other contexts are applicable. These include making code and datasets publicly accessible and subject to peer review and continuing to refine the model as additional data become available. Additional safeguards should include creating mechanisms for individuals to challenge algorithmic classifications, making classifications time limited, and using classifications to support recommendations rather than legal restrictions on individuals' movement.

Using electronic monitoring to support confined persons

Wider use of electronic monitoring to support individuals under confinement orders (isolation, quarantine, or shelter at home) should be pursued. It is aligned with both public health goals (because supported individuals are more likely to be able to stay home) and the principles of solidarity and reciprocity, which recognize societal obligations to support those called on to sacrifice liberty to prevent harm to others. Electronic monitoring is less intrusive than in-person visits by public health workers, safer for workers, and easier to scale, enabling officials to reach more people. For diseases that are only transmissible when the infected person is symptomatic, virtually observed symptom checks may speed individuals' release from confinement by quickly ascertaining when they no longer present a danger to others. Public health officials should move quickly to expand use of virtual check-ins with persons confined at home, prioritizing those most likely to need assistance because of infection status, membership in a vulnerable group, and lack of social supports.

Using electronic monitoring to enforce restrictions on movement

The use of electronic monitoring to enforce confinement orders and travel restrictions is more problematic. In the United States, for example, the Supreme Court has held that a judicial warrant must be obtained, after showing probable cause to believe a person violated the law, to search private cellphone records for law-enforcement purposes (see SM). It is unclear how courts would apply that precedent to enforcement of public health orders, but violation of some such orders is a crime.

Electronic monitoring by use of cellphone Bluetooth data, bracelets, or video cameras would likely be more effective in detecting public health order violations than current methods, which rely on police detection or police response to complaints. The question is whether more enforcement is better. The benefits of stringently enforcing mass shelter-at-home orders are not entirely clear, and the potential for strict enforcement—particularly through electronic eyes—to undermine trust in government and stoke resistance is troublesome.

The principles of the least restrictive alternative and proportionality (*7*) will be helpful in determining whether to use electronic enforcement for public health orders in future disease outbreaks. There is a strong argument in favor of monitoring bracelets for persons who present a high risk of harm to others if officials have a reasonable suspicion that they will not comply with home isolation. It is less restrictive than the likely alternative for such individuals: confining them in secure facilities. Even in this context, electronic monitoring should not immediately trigger law-enforcement action; rather, the first intervention should be outreach by public health officials. They should seek to understand the reasons for a person's noncompliance, which may include misunderstanding of the order or inability to satisfy basic needs such as food and health care.

The justification for electronic enforcement attenuates as the gravity of potential harm and likelihood of noncompliance shifts. For these reasons, population-wide shelter-at-home orders present a weak case for using electronic surveillance for individual enforcement purposes. However, using electronic data to understand the extent of compliance at the population level—as is now being done by using deidentified cellphone data to measure travel distances from home—is well justified. Such information involves little or no privacy intrusion and has helped public health officers understand whether they need to issue clarifications of what is permitted and prohibited, tighten social distancing orders further, or provide additional economic and social supports to enable people to stay home.

Using cellphone data for contact tracing

For COVID-19, the arguments for using cellphone Bluetooth data for contact tracing are

compelling. Because the virus is transmissible through casual contact for at least a few days before onset of symptoms, people are unlikely to be able to recall all those they may have exposed. Even if they could, the number of public health workers needed to perform contact tracing grossly exceeds the available supply. The most likely counterfactual is failure, or inability to fight the epidemic without longer-term social distancing orders. Digital contact tracing offers an effective, less burdensome alternative that is proportional to the threat. Not everyone has smartphones, but using the technology can conserve scarce human resources for working with those who do not.

Should the technology be installed on a mandatory, opt-out, or opt-in basis? The best available evidence suggests that for pathogens with characteristics similar to COVID-19, an opt-out regime is the least restrictive alternative. Research using UK data suggests that COVID-19 could be suppressed if 80% of smartphone users (56% of the overall population, assuming 70% smartphone penetrance) use the app (*9*). In a survey of U.S. smartphone users, about 40% said they would definitely opt in to a contact tracing app, and just under 70% said definitely or probably (figures were slightly higher for UK users) (*10*); another survey found much lower opt-in rates among U.S. smartphone users (17% definitely, 32% probably) (*11*). These numbers fall short of the mark, especially because human inertia will mean some who are willing in theory do not actually install the app. In Singapore—a small nation with fairly high tolerance for government involvement in citizens' lives—only about 20% of smartphone users have installed the TraceTogether app (*12*).

Thus, although some endorse an opt-in system (*3*), and legislation proposed in the U.S. would codify that approach (see SM), the available evidence justifies a consent regime that impinges further on individual autonomy. Bolstering the argument in favor of opt out is that users are offered reciprocal benefits: notification if they come into contact with someone dangerous and assistance in protecting friends and family whom they may have endangered.

Although some bioethicists argue that nonconsensual collection of identifiable contact data may be justified for COVID-19 to prevent harm to others (*8*), opt out is ethically preferable to mandatory use and likely to be sufficient. This setup uses choice architecture to allow those with strong preferences to act on them while not conflating philosophical objections with simple inertia. Studies of electronic health record sharing have found that people tend to stick with the default choice: Only 2 to 5% opt out of health information exchange (*13*). Although opt outs from smartphone data sharing may be higher owing to lower trust in government (*10*), opt out should be tried and evaluated before moving to mandatory use. Opt-out rates can be minimized if public health officials and technology companies collaborate to distribute plain-language FAQs that clearly explain how the data will be collected and used and what benefits there are for users.

Some propose, as an alternative, that contact tracing technology should be mandatory but have a "privacy-protecting" design in which the government receives a list of cases and a list of exposed persons but no information that permits association of particular cases and contacts (*14*). Such proposals are antithetical to effective epidemiology because they preclude use of the data to track the geographic spread of a pathogen. Use of identifiable data by governments should be carefully limited but must be permitted. TraceTogether operationalizes the least restrictive alternative principle by transmitting users' data to officials only if an individual becomes infected, and then only in specified ways. Executing binding data-use agreements can further ensure data minimization, and experts have articulated several provisions that ought to be included (*15*). Among these must be the exit strategy—plans for terminating the use of data and destroying data when the public health need for them ends (see SM).

PROCESS RECOMMENDATIONS

When any of these technologies are implemented, it should be through a thoughtful and transparent process. We endorse prior calls for an oversight process by a body that includes members of the public and focuses on particular uses of the data, not just data transfers (*3, 8*), and for "trustworthy public communication…providing transparent and convincing justifications for the decisions taken" (*7*) (see SM). South Korea and Taiwan's examples illustrate that diligent transparency can cultivate high levels of trust in the government's strategy (*2*) (see SM).

But such approaches are far from guaranteed. For example, the situation in the United States leaves much to be desired. A group of technology companies convened by the White House to discuss potential uses of technology to combat COVID-19 has no evident agenda, public or stakeholder group representation, or set of guiding principles. Ethicists and legal experts do not appear to be involved. No processes (for example, adaptation of the notice-and-comment period used for administrative rule-making) have been created for the public to give input. Proposed uses of technology have percolated up through scattered media reports but not through official channels. Communiques from companies working on these technologies are short on details about how government would be involved. No mechanisms are in place for oversight of tech companies as they pursue this work. The news media and watchdog organizations will continue to be important mechanisms for accountability, but effective oversight requires access to full information about what will be done, how, and why.

Sturdy oversight structures are not easy to stand up in the middle of an emergency. Work will be needed after the COVID-19 threat fades to ensure that we are better prepared next time. For example, federal health agencies could commission a report from the U.S. National Academies of Sciences, Engineering and Medicine recommending rules of the road for digital surveillance in pandemics, and modifications could be made to state and federal privacy and emergency powers laws to facilitate its implementation.

There has been much talk of harnessing the power and ingenuity of the tech sector to fight disease outbreaks, but "harnessing" implies carefully placed constraints and firm direction by a driver. We have yet to craft that yoke. ■

REFERENCES AND NOTES

1. D. J. Hand, *Big Data* **6**, 176 (2018).
2. C. J. Wang, C. Y. Ng, R. H. Brook, *JAMA* 10.1001/jama.2020.3151 (2020).
3. L. Ferretti *et al.*, Science **368**, eabb6936 (2020).
4. Top10VPN, COVID-19 digital rights tracker, 28 April 2020; www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker
5. S. Hendrix, R. Eglash, *Washington Post*, 19 March 2020.
6. E. Vayena *et al.*, *PLOS Comput. Biol.* **11**, e1003904 (2015).
7. Nuffield Council on Bioethics, Ethical Considerations in Responding to the COVID-19 Pandemic (Nuffield Council on Bioethics, 2020); www.nuffieldbioethics.org/assets/pdfs/Ethical-considerations-in-responding-to-the-COVID-19-pandemic.pdf
8. Nuffield Council on Bioethics, Guide to the Ethics of Surveillance and Quarantine for Novel Coronavirus (Nuffield Council on Bioethics, 2020); www.nuffieldbioethics.org/assets/pdfs/Guide-to-the-ethics-of-surveillance-and-quarantine-for-novel-coronavirus.pdf
9. R. Hinch *et al.*, Effective configurations of a digital contact tracing app: a report to NHSX (16 April 2020); https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf
10. S. Altmann *et al.*, Acceptability of app-based contact tracing for COVID-19: Cross-country survey evidence (4 May 2020); https://osf.io/6bn47/?pid=7vgq9
11. *Washington Post*/University of Maryland, National poll, 21 to 26 April 2020 (5 May 2020); https://wapo.st/3frcv3v
12. Z. Doffman, *Forbes* (12 April 2020); https://bit.ly35EQjyx
13. M. M. Mello, J. Adler-Milstein, K. L. Ding, L. Savage, *Milbank Q.* **96**, 110 (2018).
14. C. Canca, *Medium*, 10 April 2020; https://bit.ly/2YJmewn
15. Z. Emanuel *et al.*, "A national and state plan to end the coronavirus crisis" (Center for American Progress, 2020); www.americanprogress.org/issues/healthcare/news/2020/04/03/482613/national-state-plan-end-coronavirus-crisis

ACKNOWLEDGMENTS

The authors are grateful to C.-M. Chen, I-M. Parng, J.-H. Chuang, and H.-W. Jyan for generously sharing information about measures adopted in Taiwan and to G. Lo and G. Wilson for research assistance.

SUPPLEMENTARY MATERIALS

science.sciencemag.org/content/368/6494/951/suppl/DC1

Published online 11 May 2020
10.1126/science.abb9045

Ethics and governance for digital disease surveillance

Michelle M. MelloC. Jason Wang

Science, 368 (6494), • DOI: 10.1126/science.abb9045