Digital Contact Tracing for Pandemic Response

Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies, Kahn, Jeffrey P.

Published by Johns Hopkins University Press

Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance.

For additional information about this book
https://muse.jhu.edu/book/75831

For content related to this chapter
https://muse.jhu.edu/related_content?type=book&id=2628708

This work is licensed under a Creative Commons Attribution 4.0 International License.
Public health professionals around the world are working tirelessly to respond to the COVID-19 pandemic using tried-and-tested public health methods for infectious disease surveillance and control. These traditional methods are essential to the global COVID-19 response. To complement these actions and potentially augment the speed and efficacy of the public health workforce, digital technologies are being harnessed. Given the scale of the pandemic, significant efforts are being undertaken to develop and leverage public-facing and health-system-supportive technology solutions, including smartphone apps and other digital tools, that may aid public health surveillance and contact tracing.

Digital contact tracing technology and closely related digital health products (hereafter DCTT) have been used in several countries as part of broader disease surveillance and containment strategies. Globally, many digital COVID-19 contact tracing strategies have already emerged in response to the pandemic. This is not surprising given the ubiquity of mobile phones and other digital devices around the world (“Mobile Cellular Subscriptions (per 100 People)” 2018), experiences developed during prior outbreaks and pandemics, and the pre-COVID-19 momentum behind using digital technologies to support individual and health system capabilities (WHO 2017; Mathews et al. 2019; Aiello, Renson, and Zivich 2020; Mahmood et al. 2020). In the United States, DCTT has been proposed as an integral part of some plans to “reopen” the country (Allen et al. 2020; Hart et al. 2020; Simpson and Conner 2020). It is almost certain that these and related technologies will become part of not only the COVID-19 response but also the larger toolbox for future public health communicable disease prevention and control.
While novel public health surveillance technologies such as DCTT have theoretical promise, their effectiveness is unclear. These technologies also raise important ethical, legal, and governance challenges that require comprehensive analysis in order to support decision-making regarding their appropriate use. A number of frameworks, recommendations, and analyses have emerged recently in an effort to chart potentially “safe” pathways for use of public health disease surveillance technology. Many in the United States, such as the Electronic Frontier Foundation, Electronic Privacy Information Center, American Civil Liberties Union, and the Center for American Progress are proposing that digital public health surveillance technologies must embrace strict data privacy protections, decentralized data storage, a high degree of anonymity, and voluntary adoption (Crocker, Opsahl, and Cyphers 2020; Electronic Privacy Information Center 2020; Kahn Gilmor 2020; Simpson and Conner 2020). Others have argued that technologies that seek to enhance public health response during a pandemic should more closely align with the needs of public health professionals and the evidence-based procedures they follow, stating that interests in serving the public’s health ought to weigh more heavily in the necessary balancing of stakeholder interests (de Jong et al. 2019; Watson et al. 2020). This view is in part based on a recognition that during countless other outbreaks, the public has benefited from traditional disease surveillance and contact tracing, which are heavily reliant on centralized data storage and, when necessary, the collection of identifiable information. These traditional approaches are governed by ethics principles (PHLS 2002), ethics guidelines (WHO 2017), and laws (ASTHO 2012), and digital technologies represent a new tool to support them.

While debates and recommendations about appropriate design and use of DCTT have focused intensely on minimizing important data-related risks, a wider lens is needed to fully appreciate the many additional critical questions that need attention. This report begins to grapple with these questions, which are critical to address in order to guide responsible use of DCTT. Given the complexity of the terrain, as a first step toward establishing a foundation for responsible decision-making regarding potential use of DCTT, we offer a set of guiding principles (see box). These principles are meant to apply to DCTT, as well as other digital technologies used in novel ways during pandemic response.
Guiding Principles for the Use of Digital Public Health Technologies for Pandemic Response

Transparency and public engagement are essential to an inclusive digital public health response

- Government, public health, and digital technology leaders must engage effectively with the public and other stakeholders to communicate the utility, importance, oversight, and limitations of relevant digital technologies, including their implications for individuals’ privacy and civil liberties.
- Transparency at all levels is essential for maintaining public trust and confidence.
- To the extent possible, digital public health responses should reflect the range of values that are important to individuals, including advancing the health and well-being of the community as a whole.
- Decision makers should recognize the sacrifices that some people may be willing to make during a pandemic in order to advance public health goals. Acceptance by some of particular monitoring capabilities should not be read as a willingness to extend these methods to other problems or uses.

Digital public health responses must represent the least infringement of civil liberties necessary to accomplish the public health goals

- If preferred digital public health strategies infringe on privacy and other civil liberties, the infringements must be sufficiently justified by the circumstances of the pandemic, offset by ample anticipated public benefit, and considered relative to infringements associated with other possible strategies, such as mass physical distancing.
- Only those data that are necessary and relevant for the stated public health purposes should be collected. Identifiable data should be stored in a secure manner and only for the period of time that the public health purposes require.
- Adopted technologies should not be used in ways that subject communities to discrimination or surveillance for non–public health reasons.
- Respect for individual autonomy requires that users are sufficiently informed of the public health goals of the technology and the extent to which those goals are being met.

Use of digital public health technologies and data must be guided by best available evidence

- Decisions to deploy digital public health technologies should be based on a careful assessment of the uses and limitations of any proposed technology, taking into account the best available evidence.
• Those who deploy digital public health technologies should continuously and systematically monitor their performance, as well as any evidence that is being generated in other contexts about the selected technological solution and about other competing technologies.
• Unintended consequences—including those that might impact public health goals, core values and interests of the public, and unfair advantage or disadvantage—should be carefully monitored and addressed as necessary.

**Responsible use of digital public health technology requires meaningful governance and accountability**

• Systems of governance must be trustworthy and well informed. They must be reviewed and adjusted as circumstances and evidence change or as unintended effects are identified.
• Trusted representatives who are capable of developing and implementing uniform and fair standards for adopting and utilizing underlying digital technology must be identified.
• Understandable, transparent, and publicly accessible rules must guide the collection, access, control, use, storage, and combination of data by government authorities, public and private institutions, and other parties such as public health researchers.
• Oversight, accountability, and consequences for abuse or misuse of these data must be explicit and enforceable.

**The deployment of digital public health technology must be rooted in a commitment to equity**

• Digital public health technologies should be deployed in a manner that does not propagate preexisting patterns of unfair disadvantage or further distribute harms and risks unfairly throughout the population.
• To the extent possible, digital public health technologies should be designed to rectify existing inequities.
• Oversight mechanisms must be in place to ensure that the improved public health outcomes are equitable and to detect and correct any unforeseen resultant injustices attributable to the technology or that can be addressed using the technology.
• The incentives and disincentives for adopting new technology must be equitable, not exploitative, and aligned with effective use of the technology.
• Disparity-driven technology gaps should be explicitly recognized. To the extent possible, provisions should be made to address the digital divide.
In reflecting on these principles, it becomes clear that if we wish not only to realize but to *maximize* the public good that might come from use of DCTT, we must carefully define and responsibly align public health needs and capabilities with technological needs and capabilities. We must understand that although technology may serve as a workforce multiplier, it alone will not solve the public health challenges we face. We must identify and address assumptions and misinformation about technologies and data use. We must provide the means and opportunity for informed decision-making by the public and those who serve as our representatives. Government officials, public health leaders, leaders of other institutions, employers, digital technology developers, and the public all must be adequately informed and engaged in order to make the best decisions possible under the circumstances.