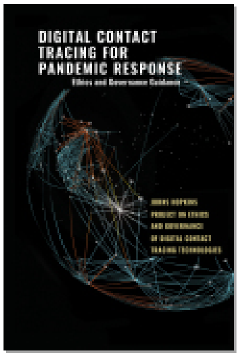
Digital Contact Tracing for Pandemic Response

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



Published by Johns Hopkins University Press

Kahn, Jeffrey and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies.
Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance.
Johns Hopkins University Press, 2020.
Project MUSE. doi:10.1353/book.75831.

Summary

Introduction

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 (together DCTT) have been used in several countries as part of broader disease surveillance and containment strategies. 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.

These technologies have significant promise. They also raise important ethical, legal, and governance challenges that require comprehensive analysis in order to support decision-making. Government officials, public health leaders, leaders of institutions, employers, digital technology developers, and the public all must be adequately informed in order to make responsible choices. Johns Hopkins University recognized the importance of helping to guide this process. It organized an expert group with members from inside and outside of Hopkins and led by its Berman Institute of Bioethics in collaboration with the Center for Health Security. Its charge was to examine the ethics, law, policy, and public health implications of using digital technologies as part of pandemic response and to develop guidance, including a framework and actionable recommendations, for governmental and institutional decision makers.

Overall, this expert group urges a stepwise approach that prioritizes alignment of technology with public health needs and public values, building choice into design architecture, and capturing real-world results and impacts to allow adjustments as required. Further, we urge an approach that recognizes that there are complicated issues to resolve for governments, institutions, and businesses and that introduction of DCTT must include public engagement and ongoing assessments to improve both performance and adoption.

Specific recommendations include the following:

- There is no “one size fits all” approach to DCTT. Technology design should not be static, but it should be capable of evolving depending upon local conditions, new evidence, and changing preferences and priorities.
- Technology companies alone should not control the terms, conditions, or capabilities of DCTT, nor should they presume to know what is acceptable to members of the public.
- DCTT should be designed to have a base set of features that protect privacy, with layers of additional capabilities that users may choose to activate. An initial default should be that user location data are not shared, but users should be provided with easy mechanisms and prompts to allow for opting-in to this capability, with encouragement to the public if it is shown to be critical to achieving public health goals.
- Data collected through DCTT should be made available to public health professionals and to researchers in de-identified form to support population-level epidemiologic analyses.

- Those who authorize use of DCTT within a particular jurisdiction or institution should continuously and systematically monitor the technology's performance in that context. This should include monitoring for effectiveness and benefit, monitoring for harms, and monitoring for the fair distribution of both benefits and harms.
- Governments should not require mandatory use of DCTT given uncertainty about potential burdens and benefits. Additional technology, user, and real-world testing is needed.

Through in-depth analysis and recommendations, this report seeks to guide decision-making and enhance understanding of

- the value of and basic methods for traditional public health surveillance and contact tracing,
- candidate technological products to enhance public health surveillance and contact tracing, and their comparative value for public health,
- core ethical, legal, policy, and governance considerations, and how they relate to relevant features of candidate technological solutions, and
- what is needed to move forward responsibly with the use of digital technology in support of public health surveillance, acknowledging gaps in our current understanding.

The full set of recommendations are intended to (1) support effective and informed adoption of DCTT, (2) encourage design of flexible technologies that maximize public health utility while respecting other values, (3) establish meaningful processes for user disclosure and authorization (consent), (4) promote equity and fairness in the uses of DCTT, and (5) foster transparent governance and oversight.

DCTT Features, Functions, and Potential Applications

Digital contact tracing technologies and platforms can be roughly categorized into three broad approaches along a spectrum of potential policies and methods: a **maximal approach** (typified by the South Korean government's centralized and triangulated data collection (M. S. Kim 2020)); a **minimal approach** (typified by the Apple/Google decentralized privacy-preserving proximity tracking (PPPT) and contact notification (Apple and Google n.d.)); and a diverse range of **middle-ground approaches** that aim to augment manual contact tracing with the collection of digital data that can be shared with public health authorities.

Minimal approaches, such as the Apple/Google PPPT, use Bluetooth Low Energy (BLE) "handshakes" that record close contact between mobile phone users but do not register the location in which the contact happened. In most architectures, these proximity data are stored in the users' phones as anonymized "beacons" that cannot be used to re-identify the users directly. If a user with a PPPT app installed on their phone tests positive and enters test results into their app, those who have been in contact with them can be notified by the app. This "exposure notification" can be automatic or at the discretion of the COV+ person, depending on the app design. If notified, a user who has been in contact with a COV+ individual would receive a push notification alerting them to possible exposure (which may be timestamped), but with no other identifying information.

The most prevalent **middle-ground approach** in the US context involves the collection and storage of personal data—including identifying information and location data—on the user's phone. These decentralized but personally identifiable data can then be voluntarily shared with public health officials if the user tests positive for SARS-CoV-2 (severe acute respiratory syndrome coronavirus 2). For example, a team at the Massachusetts Institute of Technology (MIT) has developed an app called Private Kit: Safe Paths (MIT n.d.) that stores users' location data on their phone for 28 days. If a user tests positive, she can voluntarily upload her location data to a website that is accessible only to public health officials. Officials can then analyze these personally identifiable data and, subsequently, broadcast redacted and de-identified data to other users. Healthy users would have access to these redacted location data of COV+ users, but their own data would not leave their phones. At a minimum, the storage of user location data can function as a "memory aid" if the user tests positive, but releasing the data to public health authorities may help to analyze the spread of SARS-CoV-2 and alert individuals or groups that have been in contact with COV+ patients.

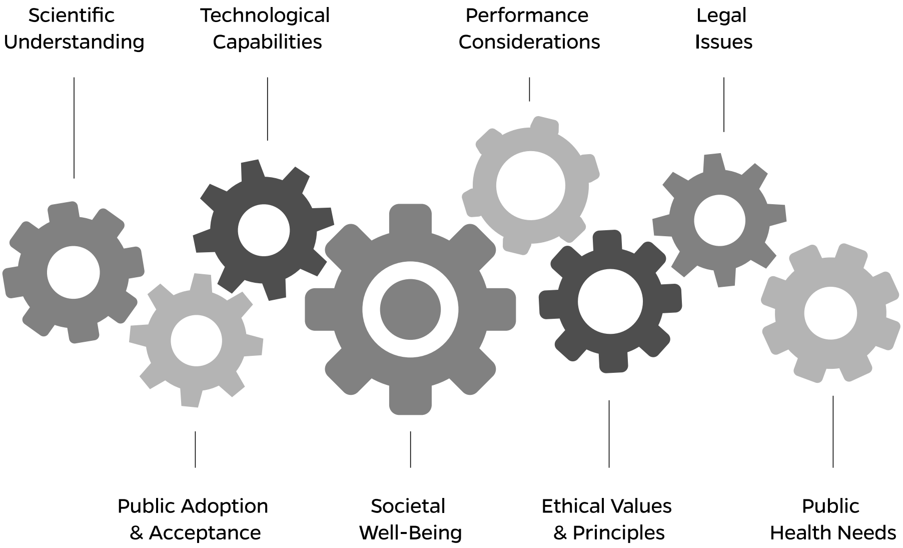

Scientific Understanding
Technological Capabilities
Performance Considerations
Legal Issues
Public Adoption & Acceptance
Societal Well-Being
Ethical Values & Principles
Public Health Needs

FIGURE 1 Interrelating Factors That Frame Responsible Development of Digital Contact Tracing Technology

The US Centers for Disease Control and Prevention (CDC) has published preliminary criteria for evaluating capabilities and attributes of DCTT (CDC 2020e). These and other resources suggest that a comprehensive assessment of DCTT and its potential to advance the public's health will require careful consideration of numerous interconnected factors that interact in complex ways and must be navigated within the challenging contexts of uncertainty and urgent need (Figure 1). These include:

- scientific and epidemiological understanding of SARS-CoV-2 transmission and infection,
- public health needs for combating the outbreak,
- technological capabilities of DCTT,
- performance of DCTT applications,
- ethical values and principles,
- characteristics of public adoption and acceptance, and
- legal issues and landscape.

The primary objectives for use of DCTT during the COVID-19 pandemic must be to reduce illness and death and facilitate public health efforts to reduce transmission of the virus. These objectives fall under a broader overall goal of contributing to societal well-being during the pandemic. It is not yet known whether and how much DCTT can contribute to these primary objectives, nor whether it will be able to contribute without generating new burdens or even harms, such as incorrect warnings or "noise" that detract from the work of manual contact tracing.

The process of identifying acceptable technology designs and uses is complex, given the interplay among the factors. Our analysis reveals that there is no "one size fits all" approach to DCTT. There is variability across the United States with respect to SARS-CoV-2 prevalence and infection rates, public health capacity, public attitudes toward DCTT, and acceptability of various potential features. Moreover, our understanding of SARS-CoV-2 and DCTT is evolving, public health response needs and capabilities are changing, and public attitudes are shifting. Different technologies used in different ways may be appropriate to achieve slightly different public health goals in different localities and at different points in the pandemic. A tiered and phased approach to technology development should be facilitated by law and policy, prioritizing underlying interoperability, while permitting user choices now and for the future.

Given the complexity of the terrain, as a first step, those developing or considering widespread use of DCTT as part of pandemic response should be guided by the following principles and related actions (see box). These principles are meant to apply to DCTT, as well as other digital technologies used in novel ways during pandemic response.

These principles make clear that in order to *maximize* the public good from use of DCTT, public health needs and technological capabilities must be carefully aligned. Government officials, public health leaders, leaders of other institutions, employers, digital technology developers, and the public are all key stakeholders that must be informed and engaged in order to enable the most successful and ethically acceptable uses of DCTT.

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.

Summary of Recommendations

The guidance document makes a number of recommendations related to (1) supporting effective and informed adoption of DCTT, (2) designing flexible technologies to maximize public health utility while respecting other values, (3) establishing meaningful processes for user disclosure and authorization/consent, (4) promoting equity and fairness in application of DCTT, and (5) instituting transparent governance and oversight. Here we provide a summary of recommendations.

Supporting Effective and Informed Adoption

- Those who authorize use of DCTT within a particular jurisdiction or institution should continuously and systematically monitor the technology's performance in that context. This should include monitoring for effectiveness and benefit, monitoring for harms, and monitoring for the fair distribution of both benefits and harms. They should also monitor evidence that is being generated in other contexts about their selected technological solution and about other competing technologies.
- Data collected through DCTT should be made available to public health professionals and to researchers in de-identified form to support population-level epidemiologic analysis.
- Data should be available to users that would permit them to further investigate their personal risk with public health officials or other health workers to add a layer of protection against unnecessary quarantine.
- Technologies or apps may produce some false negatives or false positives, but they should be accurate enough that public health authorities feel confident that they support, and don't detract from, contact tracing efforts.
- Trusted leaders should be enlisted to communicate effectively with the public about DCTT and encourage its use should the technology demonstrate some potential. The limits of knowledge regarding effectiveness should also be explained along with what will be done to improve technological capabilities as understanding evolves.

- Incentives can be a useful complement to encouragements; however, any incentives for users to install and use DCTT must be equitable, should not be coercive, and should align with effective use of the technology.
- DCTT use should not be mandated at this time given uncertainty about potential harms and benefits. Additional technology, user, and real-world testing is needed.

Designing Flexible Technology to Maximize Public Health Utility While Respecting Other Values

- Technology companies should not alone control the terms, conditions, or capabilities of DCTT, nor should they presume to know what is acceptable to members of the public.
- A "values in design" approach to development of DCTT should be adopted (Flanagan, Howe, and Nissenbaum 2008; Knobel and Bowker 2011). Robust public and user engagement activities should be pursued to identify and incorporate, to the extent possible, a range of values into the design of the technology. These values may include privacy, but also autonomy, efficiency, equity, or others. Technology design should reflect an appropriate balance and prioritization of identified values.
- Technology design should not be static, but should be capable of evolving depending upon local conditions, new evidence, and changing preferences and priorities.
- DCTT should be designed to have a base set of features that protect privacy, with layers of additional capabilities that users may choose to activate. An initial default should be that user location data are not shared, but users should be provided with easy mechanisms and prompts to allow for opting-in to this capability, with encouragement to the public if it is shown to be critical to achieving public health goals.

Establishing Meaningful Processes for User Disclosure and Authorization (Consent)

- A clear and concise module consisting of basic disclosure and voluntary authorization should be developed to accompany DCTT.

This module should not take the form of "clickwrap" terms of service or end-user agreements but rather provide only essential information necessary for an individual to make a decision. More detailed disclosures (such as FAQs in plain language) should be made easily accessible to those who wish to learn more, with no hidden surprises.

- An opt-in approach to authorization should be instituted to accompany initial DCTT rollout. The feasibility and value of opt-out approaches should continue to be evaluated, informed by what is technologically possible, what local assessments of benefits and harms of the technology reveal over time, and our evolving understanding of the degree to which an opt-out approach is likely to increase or decrease utilization among different populations. Opt-out approaches should not be precluded.

Promoting Equity and Fairness in Application of DCTT

- States, localities, and institutions that recommend widespread use of DCTT should provide technology (e.g., mobile phones, Bluetooth devices) and free data packages to those who desire but lack access to these devices.
- If there are lower rates of adoption of DCTT systems in some identifiable communities, public health authorities should find ways to compensate. For example, directing more non-DCTT resources and efforts toward those communities to meet specific needs that are elsewhere being supported by technology.
- If maps are generated based on DCTT to provide the public with the locations that COV+ individuals have visited, steps must be taken to minimize the stigma and potential financial losses that could result from a location being identified as a hotspot.

Instituting Transparent Governance and Oversight

- Digital surveillance oversight committees should be established expeditiously, with diverse and qualified membership, to provide ethical and regulatory review prior to and concurrent with widespread use of a DCTT system.
- Understandable and publicly accessible rules must guide the col-

lection, access, control, use, storage, and combination of data by government authorities, public and private institutions, and other parties such as public health researchers.

- Only those data that are necessary and relevant for the public health response to COVID-19 should be collected and used.
- Identifiable data should be kept only for the period of time needed for the public health response to COVID-19.
- Identifiable data collected as part of this response should not be shared with anyone other than the relevant public health authorities without additional specific informed consent of individual users.
- Before a government or institution adopts a digital contact tracing program, they should state the conditions under which the digital contact tracing program will be terminated.
- Future use of DCTT to advance public health or other efforts (e.g., use in seasonal flu surveillance) would require independent justification. DCTT designed for public health use should not be used by law or immigration enforcement.
- The principles offered in this guidance document apply both during and following the COVID-19 pandemic.

Legislative Recommendations

- The United States Congress should enact new legislation, specifically tailored to facilitate the use of DCTT as part of the public health response to COVID-19, while also protecting user privacy and ensuring data security.
- Congress should require DCTT developers to disclose to users, in clear language, the nature of the information that would be collected, how it would be collected, how it would be stored, and for what purposes it may be used.
- While the rollout of DCTT should initially employ an opt-in authorization approach, the feasibility, acceptability, and value of opt-out approaches should continue to be evaluated. As such, opt-out approaches to consent should not be precluded by legislation.

- Congress should prohibit the commercial use of data collected for COVID-19 response by DCTT.
- Congress should prohibit discrimination on the basis of data collected by DCTT.
- If Congress is unable to enact suitable legislation, state legislatures should work toward enacting similar laws for their jurisdictions. A "model" state law should be rapidly developed to facilitate nationwide adoption of an appropriate law and uniformity of legal requirements.

Summary of Analysis

Supporting Effective and Informed Adoption

The COVID-19 pandemic and the physical distancing efforts implemented to slow the rate of transmission have caused severe harm to individuals, communities, and our society. To protect the public good going forward, we need a robust public health response that reduces the spread of SARS-CoV-2 and does so in a way that allows economic recovery to occur and to be sustained. We also need to design and manage this public health response so as to minimize harms to individuals and society, to distribute benefits and burdens equitably across the population, and to avoid misuses of the technologies and the data they collect.

To reduce the spread of SARS-CoV-2, chains of transmission need to be broken. To do this, people who have been exposed to SARS-CoV-2, or potentially exposed, need to be identified as comprehensively and as quickly as possible so they can quarantine themselves and avoid infecting others. This is the job of manual contact tracing by public health authorities, in which people infected or presumptively infected with SARS-CoV-2 are interviewed and asked about their movements and interactions, including where they work and shop, how they travel, with whom they've had contact, and the nature of that contact (e.g., where the contact took place). Their contacts are then interviewed and potentially asked to quarantine, seek testing, and take other protective measures if the contact is sufficiently high risk.

The hope is that DCTT can augment traditional contact tracing efforts, either by working alongside and independently of manual contact tracing or by being integrated into manual contact tracing efforts in a way that makes these efforts faster, more thorough, and more efficient.

Data suggest that a substantial proportion of transmissions—perhaps as high as 50%—occur between individuals who are not symptomatic and that transmission may occur as early as 3 days before onset of symptoms (WHO 2020). Because asymptomatic spread of SARS-CoV-2 appears to be a significant source of infection, we need to identify potentially infected people before they show symptoms; thus, speed is of the essence. This is one benefit of using DCTT: potential contacts can be identified instantaneously, notified quickly, and asked to quarantine as soon as possible.

Another benefit is identifying contacts who manual contact tracing methods may miss, either because COV+ people do not remember all the places they've been or cannot identify all the people they've had contact with. This is especially relevant given the long period of infectivity of SARS-CoV-2, which begins before people are symptomatic and aware they are infected (Ferretti et al. 2020). If DCTT were designed to have optional location-monitoring capabilities, this critical challenge could be mitigated even further. For example, location data might reveal that a COV+ person was at a restaurant at an exact time and date, which could be followed up by contact tracers who could alert the public or use other measures to reach those who were also present in the restaurant at the same time. In other disease contexts, geolocation data have demonstrated some potential to support epidemiology and disease surveillance (see Furlanello et al. 2002; Dredze et al. 2013; Eckhoff and Tatem 2015; Fraccaro et al. 2019), with technical cautions regarding accuracy and the like (Beukenhorst et al. 2017).

One role for DCTT is to work alongside manual contact tracing but independently of it. Individuals would download proximity tracing or exposure notification apps, use them, receive alerts if they've had a potential contact with another user who is COV+ or presumptively COV+, and voluntarily self-quarantine without having contact with public health authorities or giving them data that feeds into public health contact tracing efforts. It is possible that this would help to break chains of transmission and reduce the spread of SARS-CoV-2, though at this point these benefits are speculative. It is also possible that such exposure notifications will result in high rates of false positives.

Another possible role is for DCTT to be integrated into manual contact tracing efforts. When potential contacts are identified by DCTT, they are connected to public health authorities who can then follow up with them. There are different forms this could take and different kinds and amounts of data about contacts public health authorities could receive from DCTT. On one end of the spectrum of reporting, public health authorities would not receive individuals' names or contact information, only anonymous data. The fullest version of reporting would securely send to public health authorities the names, contact information such as address and phone number, and other data about contacts that DCTT collected, including data about their location and movement history.

It is uncertain whether providing public health authorities with volumes of information on cases and contacts from DCTT will be useful in practice. As mentioned above, providing public health authorities with location data on cases and contacts collected by DCTT may help contact tracers to find and notify additional contacts. However, at present, providing public health authorities with large amounts of data will be useful only if there is sufficient capacity to follow up on these data. In addition, there is a risk of low-quality data from DCTT flooding the system, leading to investigation of false case contacts identified by DCTT and distracting from other important efforts. Whether and to what extent data from DCTT will benefit contact tracing efforts is unknown, pointing again to the importance of continuously collecting high-quality evidence about DCTT.

Designing Flexible Technology to Maximize Public Health Utility While Respecting Other Values

Use of DCTT is essentially an experiment, as we have insufficient information about the performance of different DCTT and their efficacy. In the face of this uncertainty, how should DCTT be designed and how should its use be managed?

Many efforts to advance DCTT in the United States and elsewhere have emphasized the importance of "privacy by design"; that is, building privacy and security protections into the design of technology rather than counting on responsible use alone (Cavoukian 2010). As noted above, some major technology companies have signaled this position through development of PPPT systems that embed features such as decentralization, de-identified information, user anonymity, bans on collection of location data, and minimal reliance on or integration of public health authorities or other government actors. Many of these features have also been embraced early by advocacy organizations (Crocker, Opsahl, and Cyphers 2020; Electronic Privacy Information Center 2020; Kahn Gilmor 2020) and in an open letter ("Joint Statement on Contact Tracing" 2020) from nearly 300 researchers. These same actors have emphasized that use of DCTT should be fully voluntary.

Although privacy is a key value, individuals and communities may also value efficiency, equity, liberty, autonomy, economic well-being, companionship, patriotism, or solidarity, among other values. People may accept more significant encroachments on privacy now if this ultimately results in realizing other values (such as companionship) that are of equal or greater importance to those individuals. Rather than centering privacy alone in design, a different orientation is needed at this moment: that of "values in design," which incorporates a broader range of values into technology (Flanagan, Howe, and Nissenbaum 2008; Knobel and Bowker 2011). For example, some users might wish to express autonomy, solidarity, or patriotism through DCTT by sharing their location history with public health professionals in order to advance the public health response, increase system efficiencies (e.g., by contributing information that can lead to better data processing), and reduce the burden on essential workers. At the same time, there is value in further advancing autonomy by designing technology to allow individuals some control over what data about them are collected and shared.

DCTT should be designed to have a base set of features that protect privacy and strive for interoperability, but also should include other optional capabilities. This could be achieved by designing DCTT to have a default that can be modified: for example, an initial setting could be that users' location data are not shared with public health authorities, but users may opt-in to this feature. Such an opt-in approach is likely consistent with existing federal privacy laws.

Designing DCTT this way gives users the flexibility to decide how to use the technology and how to engage with public health authorities, consistent with their values and trade-offs they are willing to make. This flexibility could also allow for more real-world evaluation of how different users experience different features of DCTT in different locations. Technology design should not be static, but it should be capable of evolving depending upon local conditions, new evidence, and changing preferences and priorities.

DCTT developers must comply with a number of federal privacy laws. These privacy laws generally permit the collection, storage, and use of personal information, so long as the user provides meaningful consent. Privacy law in the United States is generally sector-specific and limited in scope, resulting in a patchwork of protections that differ significantly depending on the entity that collects the data and the type of data collected. Given the complexity of existing federal privacy law and the need to further strengthen public trust in DCTT, it would be beneficial for Congress to enact new privacy legislation that is specifically tailored to the use of DCTT in response to COVID-19. Such COVID-specific legislation should be sensitive to the full range of values and recommendations described above.

In short, designing "middle-ground" DCTT for flexible use may provide the most adaptable and thus most robust public health response—respecting privacy and individual autonomy by allowing users to use DCTT in ways that express their own values.

Public Acceptance of DCTT

While some groups have maintained that only PPPT-like minimal systems will be widely adopted, because only they will earn and maintain public trust (Simpson and Conner 2020), there is insufficient evidence that public trust would be threatened by a DCTT system that has the capacity to securely collect location data, integrate public health authorities, and enable voluntary sharing of certain user data (e.g., location data) with those authorities. More research, including through deliberative engagement sessions, is needed to better understand how differences in the features and functionality of DCTT (such as optional sharing of geolocation data) influence trust and people's willingness to use DCTT. Technology companies should not alone control the terms, conditions, and capabilities of DCTT, nor should they presume to know what is acceptable to members of the public.

Significant concerns have also been expressed by privacy advocates (Guariglia 2020) and in the popular press (Giglio 2020) about "surveillance creep"—that is, a belief that state or corporate actors will use new surveillance technologies, capacities, and permissions well beyond the purposes for which they were initially justified to the public and beyond the time when they are useful for the COVID-19 pandemic. Surveillance creep is a serious concern and should be carefully guarded against; however, the possibility of surveillance creep is not a sufficient reason to limit development of DCTT to minimal systems. Instead, protections should be put in place to ensure that only those data that are necessary and relevant for the public health purposes at hand are collected and used, and data should be kept only for the period of time needed for those public health purposes. For this reason, we would support COVID-specific legislation that would impose strict limits on the use of DCTT data for non–public health purposes.

Finally, the use of DCTT during the current pandemic should not set a precedent for future public health use (e.g., use in seasonal flu surveillance efforts). Future use would require independent justification. Further, use of DCTT in other contexts (e.g., by law enforcement or immigration enforcement) is presumptively unethical.

Encouraging Adoption of DCTT

Researchers have estimated, perhaps conservatively, that DCTT use by 80% of smartphone owners, or 56% of the population overall, will be needed to suppress the epidemic (Hinch et al. 2020). These estimates also highlight that some decrease in transmission would be realizable even with lower rates of technology adoption.

In the United States, many advocates and researchers have argued that use of DCTT must be fully voluntary. However, experience from other countries suggests that when use of a digital contact tracing app is voluntary, only a minority of the population will download it. Instead of making use fully voluntary and initiated by users, there are ways that DCTT could be put into use without users' voluntary choice. For example, use of an app could be mandated as a precondition for returning to work or school, or even further, to control entry into a facility or transportation (such as airplanes) through scanning of a QR code to demonstrate personal exposure levels (Gan and Culver 2020).

While these approaches are hard to imagine in the United States, some have argued that mandatory use of DCTT could be ethical. If mandates increase adoption of DCTT and improve the public health response, this would reduce the likelihood of lockdowns, which are harmful and a severe limitation of individual liberty applied on a mass scale. On the other hand, mandated use of DCTT systems may not be effective. People may not adhere to the mandate by simply leaving their phone at home. Perhaps more important, should the technology not deliver the hoped-for benefits, having mandated the use of an unproven technology could result in a loss of public trust in the technology, in the entity instituting the mandate, and in the larger public health response, potentially leading to noncompliance with public health recommendations more broadly (Bernstein et al. 2019).

Any decision maker considering mandatory use, including government officials, institutional leaders, and employers, must convincingly address a number of considerations. Particularly important is the need to identify reliable evidence that the DCTT would be effective and to ensure that the burdens and benefits of use are equitable and justifiable. At this time, mandated use of DCTT by states or institutions is not justifiable given uncertainty about potential harms and benefits. Additional technology, user, and real-world testing is needed before mandatory use should be considered.

As with any public health effort, the amount of evidence that must be offered to illustrate that the intervention or program can achieve its aims, and the degree to which people should be able to exercise choice in their participation, should be in proportion to the anticipated burdens of the intervention or program. For example, the permissibility of mandating use of DCTT by the public depends on factors such as the sensitivity of the data that are collected, the extent to which public health is integrated within the DCTT system, and what actions are taken in response to confirmed virus exposure or being identified as COV+ (e.g., forced quarantine). The more burdens that are placed on individuals—for example, whether people are ordered into quarantine if they have been exposed to the virus, or if there are limited social supports for those in quarantine—the greater the demand should be on the performance of the DCTT system.

Perhaps the most effective way to generate widespread US adoption of DCTT will be to offer incentives for its use; in other contexts, generally speaking, small incentives have been shown to lead to an increase in desired outcome (Singer and Ye 2013; Lee et al. 2014). Given the importance of widespread use, modest incentives ought to be considered if and when there is sufficient evidence of the utility of DCTT, so long as those incentives are not mandates in disguise. Another "first line" approach to increasing use of DCTT is for trusted community leaders, public figures, health care professionals, and other respected individuals to communicate with the public and their communities about DCTT and to encourage its use through public engagement campaigns, if and when the technology demonstrates sufficient potential.

Establishing Meaningful Processes for User Disclosure and Authorization (Consent)

Any effort to roll out DCTT should ensure that users have a meaningful opportunity to review and understand information about the specific technology and its uses. Moreover, given the importance of public trust and the current crisis of public trust in governments and technology companies handling private digital information, there is a strong ethics argument for requiring consent from individual users. We recommend a carefully crafted version of what is sometimes called simple consent, which consists of basic disclosure and voluntary agreement or authorization. This disclosure should include information about the purposes of the technology, the user's options for collecting and sharing data, purposes for which data can be used, and any known risks, among other information. This information should be presented in an accessible format on any DCTT app, and more detailed disclosures should be readily accessible for those who wish to review them.

Through an opt-in mechanism such as clicking a button to signal agreement, users should be able to indicate their intention to use a DCTT. The opt-in approach is consistent with mechanisms for agreement to use other downloaded applications. An opt-in approach should be part of the initial introduction of DCTT given the novelty of the technology and its uses and the need to build trust and confidence in the system. Successes of opt-out approaches in other areas suggest that the feasibility and value of an opt-out approach to DCTT should be carefully evaluated, particularly in conjunction with assessment of whether public health goals are being met (Rithalia et al. 2009). Such assessments should be informed by what is technologically possible, by local data regarding benefits and harms of the technology, and by evolving understanding of the degree to which an opt-out approach is likely to increase or decrease utilization among different populations.

Promoting Equity and Fairness in Application of DCTT

Digital contact tracing technology should be designed and used in ways that, as far as possible, promote an equitable distribution of benefits and burdens. DCTT should be deployed in a manner that does not propagate preexisting patterns of unfair disadvantage or distribute harms and risks unfairly throughout the population. It is well known that some communities have lower rates of technology and data access, and therefore may benefit less from use of DCTT unless steps are taken to address these digital disparities. Additionally, should use of DCTT be made a requirement for entry into a workplace, into a school, or onto transportation, then those who currently do not possess the required technology must not be unfairly burdened through lack of access. In order to mitigate this, states, localities, and institutions that recommend widespread use of DCTT should provide technology (e.g., mobile phones, Bluetooth devices) and free data packages to members of the community who desire but lack access to these devices.

Some populations may also experience greater harm, and greater fear of harm, from having their data collected. For example, some groups such as African Americans, Hispanic Americans, Muslim Americans, and undocumented immigrants have more reasonable fear of their data being handed over to law or immigration enforcement, and some groups have lower levels of trust in public health due to past injustices (Auxier et al. 2019; CSM 2017; Pew Research Center 2017; Rodrigues et al. 2018). This further substantiates the need to limit use of any data gathered by DCTT to its public health purpose.

Instituting Transparent Governance and Oversight

DCTT must be developed with an eye toward both present and future implications. We are rapidly gaining knowledge about SARS-CoV-2 and COVID-19, but still have essential gaps in our understanding. In the United States, public health responses including DCTT will generally be developed and coordinated by individual states, regional consortia (Reston, Sgueglia, and Mossburg 2020) and associations. Good governance in this context requires transparency and the creation of oversight bodies with the appropriate expertise and representation to allow nimble and effective responses while serving as trusted representatives.

In order to address the range of ethics and governance concerns that relate to the design and use of DCTT, we recommend that digital surveillance oversight committees be established, perhaps at a state level and with a platform for national coordination. These committees can provide ethics and regulatory review prior to and concurrent with widespread use of DCTT. The committees should be composed of a diverse group of experts capable of evaluating the quality of a DCTT system locally, including members of communities that experience higher rates of digital disparity.

When assessing the design and use of digital contact tracing systems, these committees (and the public more widely) should consider not only the risks and benefits accrued during the COVID-19 pandemic but also implications for the future. How can we navigate safe use of these technologies in a way that preserves public trust in them and enables the possibility of future beneficial use?

As a start, it should be emphasized that the principles offered in this and other guidance documents do not apply only during the pandemic. Future efforts to advance DCTT capabilities, during quieter times, should make every effort to follow them.