3. Ethics of Designing and Using DCTT

Published by


⇒ For additional information about this book
https://muse.jhu.edu/book/75831
Those developing DCTT, and those considering its use, should systematically take into account and document alignment with the guiding principles outlined in this report.

When considering the ethics of DCTT, key ethical questions concern the features that DCTT should have (e.g., should digital contact tracing apps collect users’ location data?), whether and how individuals’ data should be shared with public health authorities, how ethically to encourage use of DCTT (e.g., under what circumstances would it be ethical to incentivize or mandate use of DCTT), what kind of supports and equity-promoting measures should accompany use of DCTT, and how governance and oversight of DCTT should be structured.

The sections that follow consider these questions one by one. A key conclusion of this report is that these features of the design and use of DCTT are ethically interrelated—reaching a determination regarding any one question requires careful consideration of them all. Rather than reaching “one size fits all” conclusions about specific features of uses of DCTT, decision makers should ethically assess DCTT systems holistically.

Generally, a public health measure is ethically justifiable if it strikes a reasonable balance between competing considerations and if it provides sufficient public health benefit (or the prospect of benefit) to justify the burdens associated with it. DCTT systems are ethically justifiable if they strike a reasonable balance between multiple ethical considerations including:

- enabling an effective and efficient public health response,
- protecting individual privacy and preventing harms to individuals,
including harms from sensitive data being revealed and from erroneously being subjected to isolation or quarantine orders,

- allowing individuals to control what information about them is collected and revealed to whom, including through appropriate disclosure and authorization processes for data collection,

- promoting equitable distribution of benefits and burdens of DCTT,

- maintaining public trust in DCTT and in the COVID-19 public health response, and

- taking seriously the future implications of decisions that we make today.

To illustrate a holistic assessment, consider whether it is ethically justifiable for an employer to mandate that employees use a DCTT as a condition of returning to work. This will depend upon many features of the DCTT system: what kind of data the DCTT collects (e.g., does it collect location data or just record proximity events); whether there is public health capacity to make good use of these data; what the data are used for (e.g., will the employer ban an employee from the workplace on the basis of a DCTT-identified contact?); what kind of social supports are available (e.g., is there paid leave for employees?); what employees’ attitudes are toward use of DCTT; and whether mandating use is likely to have public health benefit, among other factors. These factors may vary from place to place and may change over the course of the pandemic. Thus there is no “one size fits all” ethically optimal approach to DCTT.

Justifying the Use of DCTT Systems

A foundational issue is why deploying any DCTT during a pandemic is justified, given there are manual contact tracing capabilities that are well established, while the performance and effectiveness of novel technologies is less established. The need to move quickly to minimize the spread of the virus poses challenges here, as the data needed to fully make the case that these technologies substantially contribute to the public health response may not be available prior to widespread use. The primary argument for DCTT is that the capacity of manual contact tracing may be
exceeded, and we may not be able to bolster the public health workforce rapidly and sufficiently enough to meet needs. DCTT has the potential to quickly and exponentially expand the reach of contact tracing. In addition, DCTT may allow more efficient identification and quarantine of potential contacts of COV+ people than manual contact tracing alone, particularly given the high number of infections that have been spread by asymptomatic individuals.

Nonetheless, reasonable people disagree about the prudence of pursuing DCTT, especially given its limited performance history and potential risks, including diverting attention and resources from more effective interventions. The limited attention and resources available during a pandemic must be allocated efficiently and effectively.

To justify potentially widespread use of technologies such as DCTT, therefore, a number of considerations must be addressed:

• whether the technology is designed to meet an important and unmet public health need,
• whether there is sufficient evidence or reason to suggest that the technology will be effective at serving its purpose,
• whether the outbreak is characterized by sufficiently severe morbidity and mortality and a high rate of disease transmission to warrant large-scale introduction of novel systems,
• whether there are other less autonomy-restricting or less risky alternatives to widespread use, and
• whether it is reasonably likely that a sufficient number of individuals will use the technology to achieve the intended public health benefit.

**Monitoring and Evaluating Technologies to Inform Policy and Practice**

A number of public health ethics principles necessitate the ongoing monitoring and evaluation of DCTT systems. First, DCTT must be shown to perform reasonably well at achieving its stated goal: reducing the spread of SARS-CoV-2. The effectiveness of DCTT programs should be illustrated at a number of stages.
1. Robust initial technology testing is needed to publicly justify the widespread adoption of DCTT and avoid public failures, which may hamper future uptake (e.g., Lovejoy 2020; Morse 2020). This typically includes alpha testing in virtual environments and beta testing in different community settings.

2. If and when a DCTT is implemented on a wide scale, it must be monitored on an ongoing basis to assess reach, effectiveness, functionality, best practices, and any harms.

3. When approaching a previously identified stopping point for use of DCTT, monitoring can help to identify when utilization is no longer needed.

If at any of these points evidence clearly suggests harm (particularly in comparison to other methods that the public might find more acceptable), this evidence should provide a basis upon which to revisit strategies, priorities, and allocation of resources. Attention should be given to foreseeable side effects that may dramatically influence the overall effectiveness of the program, such as individuals carrying their smartphones around with them selectively so as to avoid particular undesired consequences of DCTT policies.

Anonymized aggregate data, including user feedback, must be evaluated to ensure that benefits and burdens are distributed fairly. As noted earlier, unintended burdens may include inequitable outcomes that may arise in a DCTT program; for example, resulting from uneven access to the required technology to participate, disparate concerns about surveillance within some communities that might limit widespread use, or discrimination that may result from being identified as COV+ due to the program or for communities that are termed “hotspots” based on maps of COV+ location data. Additionally, it is possible that some communities might get higher rates of false positives because they are located in densely populated areas, thus increasing the burden of self-isolation. If any of these inequities are identified, steps must be taken to mitigate them.

Finally, numerous actors should engage in the monitoring and evaluation of DCTT systems. Technology developers and public health researchers have a clear role in this process. Technology developers should work with public health researchers to monitor accuracy, precision, func-
tionality, confidence of estimates, sources of error, and the like. Researchers may also be able to contribute innovative methods to systematically and rapidly evaluate candidate technologies, such as by deploying cluster randomized stepped wedge (Hemming et al. 2015) or adaptive trial designs and techniques (e.g., response-adjusted randomization) (Pallmann et al. 2018). These approaches were also proposed for use in research to assign candidate experimental treatments and vaccines during the 2014-15 Ebola outbreak (Berry et al. 2016). When formal research activities are pursued, ethics principles and legal requirements for the conduct of research should apply (e.g., The Belmont Report).

Furthermore, any workplace or institution that incentivizes or mandates use of DCTT has a responsibility to provide evidence that the intervention, at minimum, is not likely to cause harm and to monitor for unanticipated burdens. In all cases, it is vital that a trusted intermediary be involved in the evaluation of DCTT programs to limit perceptions of bias and ensure a legitimate basis for decision-making. Nonsensitive aggregate DCTT analyses should be made available to the public so as to permit verification and inform continuing public debates about its usefulness and necessity. At an individual level, data should be available to users that would permit them to further investigate their personal risk with public health officials or other health workers. This is important not only to ensure their health and well-being but also to add a layer of protection against unnecessary quarantine.

**Recommendations**

- Reviews of DCTT systems must be conducted in part by an independent intermediary that has established the public’s trust.

- 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 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.

Public Trust and Public Attitudes

Researchers have estimated, perhaps conservatively, that DCTT use by 80% of smartphone owners—56% of the population—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. As such, in order to maximize impact, it is essential to gain a thorough understanding of public perspectives on DCTT, including which features and uses of the technology the public finds acceptable, which kinds of DCTT the public would be most likely to use, and which designs and uses of DCTT would maintain or jeopardize public confidence and trust. There will be variation in public attitudes within and across societies and over time.

With respect to what we currently know about public attitudes and trust in DCTT in the United States, polling data suggest some potential support and also some divisions regarding willingness to use the technology. Polls conducted by groups based at the University of Zurich (Hargittai et al. 2020) and the University of Oxford (Altmann et al. 2020) suggest that more than 60% of Americans would be willing to install such an app. Both a Washington Post–University of Maryland poll (2020) and a Kaiser Family Foundation poll (Kirzinger et al. 2020) show roughly half of the population would be willing to install the app. Over half of the population (59%) would be willing to share their COVID-19 positive test result with an app in order to anonymously share that information with their contacts (Washington Post–UMD 2020). Only 29% of respondents to a March 12–27 Oliver Wyman Forum poll (Elliott et al. 2020) said that they would be willing to share their location data. Additionally, Washington Post–UMD data and Pew data from 2019 suggest that approximately one in six Americans do not have a smartphone and thus cannot use the technology without intervention (Pew Research Center 2020).

People may be more willing, however, to download an app if it will
ease social distancing policies and allow for more economic and social activity. Willingness to install a contact tracing app increased among respondents to the Kaiser Family Foundation poll from 50% to 66% when respondents were asked if they would be willing to do so to allow schools and businesses to reopen. Additionally, who develops or administers the app appears to matter. Respondents to the Washington Post–UMD poll indicated higher levels of trust that their anonymity would be preserved by public health agencies and universities than by tech companies or health insurance companies. Further, more respondents to the Oliver Wyman Forum poll were willing to share their health information with public health authorities (55%) than the local government (35%), their employer or school (33%), or the federal government (27%).

These data suggest that people will be more willing to use a contact tracing app when the potential benefits are clearly identified and valued, such as lifting social distancing measures, and they will be more willing to do so if the data are going to a public health agency rather than the federal government or a tech company. Other factors that seem to be associated with greater willingness to install a contact tracing app include younger age and the app source (Hargittai et al. 2020), with a preference for apps distributed by public health agencies over others such as health insurers or public universities (Hargittai and Redmiles 2020). However, all of this must be read with caution, as public polling may not be representative of some populations or of widespread public attitudes. Further, these attitudes may shift over time and may be discordant with behaviors (Barth and de Jong 2017).

Deliberative public engagement efforts would be an appropriate means of filling in gaps in understanding about the acceptability of different approaches (Fishkin and Laslett 2003; Cavalier 2011). In addition, including the public, particularly in the earlier stages of planning a path to sustainable resolution to the pandemic, could serve to help disseminate a nuanced understanding of what is at stake, including the key challenges and trade-offs. Aggregated public polling results are not sufficient as a proxy for careful analyses of the ethical challenges; but, they do provide a necessary input for these analyses. Integrating lessons and outputs from public engagement into guidance and other products requires special attention and should be validated and enhanced through further engagement.
Recommendations

• More research into public attitudes is needed. In particular, in-depth qualitative research should examine public attitudes about perceptions of trust in DCTT among different communities, which features of DCTT influence trust, and the extent to which people are willing to provide different types of data through DCTT to help their community.

• States and localities that are considering adopting DCTT should engage with the public to increase their understanding of the acceptability of DCTT design features and uses among diverse communities.

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

Values in Design

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 decentralized privacy-preserving proximity tracking (PPPT) systems. These systems embed features such as decentralization, anonymity of users, 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 from nearly 300 researchers (“Joint Statement on Contact Tracing” 2020).

Privacy by design provides principles that incorporate one set of values (privacy) into the design of DCTT. Importantly, the principles acknowledge the need to design privacy defaults into systems, while maintaining the capacity of those systems to achieve their otherwise justifiable ends. Put another way, privacy by design “embraces legitimate non-privacy objectives and accommodates them, in an innovative positive-sum manner” (Cavoukian 2010, p. 4).
This stance, simple in its statement, is not easy to satisfy. Given that “objectives” are themselves driven by values, it begs for an articulation of additional values (aside from privacy) that individuals and groups within society—including many privacy advocates—may believe to be important. For example, at any moment, in addition to valuing their own privacy, individuals may value efficiency, equity, autonomy, economic well-being, companionship, patriotism, or solidarity. Moreover, the above stance necessitates an acknowledgment that peoples’ value priorities often change when circumstances change, not least of which during a pandemic when mass physical distancing has made it difficult to fully realize many important values (aside from physical privacy). A different orientation is needed at this moment. As Flanagan, Howe, and Nissenbaum (2008) conceptualized in 2008, we should take a “values in design” approach to DCTT—an approach that designs a broader range of values, such as those enumerated above, into technology.

This approach requires a wider ethical lens through which to examine DCTT and requires hard but important work to appropriately balance competing interests within technology architecture. For example, there is value in technology providing users the option to collect their location history and share it 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. For some, this might be an expression of autonomy, solidarity, or patriotism. At the same time, there is value in further advancing autonomy by designing technology to allow individuals to control what data about them are collected and shared.

**Justifying a Middle-Ground Approach to DCTT**

We ought to embrace a DCTT that has a default of interoperability and privacy protection, but that does not stop there. Triggering events, such as entry of a positive test result or receipt of a notification that one was proximate to someone who tested positive, could, for example, generate a push notification that users can acknowledge in order to permit transmission of potentially useful location data to public health authorities. This could be accompanied by an explanation of the value of the information and relevant restrictions on its use.

At this point, it is worth reiterating that manual contact tracing—
which involves collecting information from people who’ve tested positive and their contacts—includes collection of personal information and potentially embarrassing or sensitive data about the places they’ve been and the people they’ve had contact with. Manual contact tracing efforts use these data to uncover ongoing transmission, provide useful information tailored to the individual, and enable isolation and quarantine as necessary.

It stands to reason that if these forms of data can be collected by a DCTT and provided to public health authorities in a maximally secure and voluntary way (with clear rules regarding authorized uses), this may amplify public health authorities’ manual contact tracing efforts. For example, location data from DCTT could help jog people’s memories about where they’ve been and fill in memory gaps. This is especially relevant given the long period of infectivity of SARS-CoV-2, which begins before people are symptomatic and therefore before they are aware they are infected (Ferretti et al. 2020). 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 (see Furlanello et al. 2002; Dredze et al. 2013; Eckhoff and Tatem 2015; Fraccaro et al. 2019), geolocation data have demonstrated some potential to support epidemiology and disease surveillance, with technical cautions regarding accuracy and the like (Beukenhorst et al. 2017).

These benefits are currently speculative for DCTT. At present, providing public health authorities with large amounts of data on cases and potential case contacts will be useful only if there is sufficient public health capacity to follow up on these data. In addition, there is a risk of low-quality data from DCTT flooding the system. Investigating potential case contacts identified by a DCTT may distract them from other important efforts and at some point overwhelm public health capacity altogether. 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.

Nevertheless, what would enable the most flexible and potentially robust public health response is to design DCTT so that restricted data sharing is possible. From an ethics perspective, the collection and use
of sensitive data in manual contact tracing efforts (described above) is typically seen as ethically justifiable so long as there is sufficient public health benefit and need. Thus, wouldn’t it seem appropriate from both a public health and ethics perspective to design DCTT systems to enable similar data to be shared with public health authorities when and if there is ethical justification for sharing them?

Why, instead, do so many advocate that DCTT should be designed as a “minimal” system, when this arguably ties the hands of public health and individual users and precludes the collection of data that public health authorities (and indeed many other apps on our phones) typically collect? We here consider, and appraise, some of the reasons that may motivate individuals and groups to argue for minimalistic positions:

1. **Proponents of minimal systems may believe that such systems will be most widely adopted.** Some groups have maintained that only these systems will earn and maintain public trust and be widely adopted (Simpson and Conner 2020). For example, the previously referenced open letter (“Joint Statement on Contact Tracing” 2020) asserts: “Some of the Bluetooth-based proposals respect the individual’s right to privacy, whilst others would enable (via mission creep) a form of government or private sector surveillance that would catastrophically hamper trust in and acceptance of such an application by society at large. It is crucial that citizens trust the applications in order to produce sufficient uptake to make a difference in tackling the crisis. It is vital that, in coming out of the current crisis, we do not create a tool that enables large scale data collection on the population, either now or at a later time. Thus, solutions which allow reconstructing invasive information about the population should be rejected without further discussion.”

   **Response:** While it is true that public trust in and acceptance of DCTT is essential for its success, there is insufficient evidence that public trust would be threatened by a DCTT system that has the capacity to collect location data and enable voluntary sharing of those data with public health authorities. A contrasting perspective is that maintaining public trust requires maintaining public confidence that the DCTT system is providing useful information, is benefiting and not harming individuals, and is advancing the
public health response (Leprince-Ringuet 2020). From this perspective, a system that is less well integrated into the broader public health response, or that generates a higher rate of false positives (as some suggest decentralized approaches might (Fraser et al. 2020)), may fare worse when it comes to maintaining public confidence and trust.

2. **Proponents may hold the view that minimal systems are harmless (or nearly harmless) to individuals.** This is because individuals are anonymous, none of their location data are gathered, and none of their identifiable data are shared with anyone. In contrast, DCTT systems that collect and share identifiable data, including location data, may be seen as posing risks of harm to individuals.

**Response:** While minimal systems may be harmless (or nearly harmless) from the perspective of protecting privacy, they may not be harmless from the perspective of public health if they generate system inefficiencies through producing too many false positive or false negative contacts. Aside from presenting a challenge for public health professionals, false positives could also harm individuals. If users receive a large volume of automated messages alerting them to proximity events, will this cause distress? Will a large volume of alerts cause users to become disengaged and stop using the DCTT or lose confidence in contact tracing more generally as a legitimate method of disease control? Admittedly, these are just potential harms and risks; it is unknown the degree to which they will materialize. The point is that privacy-related harms are not the only relevant harms to individuals that we should consider when assessing DCTT.

We acknowledge the risk under a middle-ground DCTT of data being used in ethically unjustifiable and harmful ways. For example, it would be against the principles and recommendations articulated in this report for data to be sold or monetized by technology companies or others for corporate gain, and this misuse of data would be more intrusive if the data were potentially identifiable. What makes it ethically justifiable to take this risk is the compensating benefit of allowing the most flexible and robust public health
response during the pandemic, but this alone is not sufficient. The risk of inappropriate uses must be reduced by ensuring stringent requirements for data security and access, as well as clear legal protections and recourse for any violations (as discussed further below).

3. **Proponents may believe that DCTT systems should not collect location data as this would be too intrusive and of insufficient value.** Some proponents of PPPT systems maintain that recording proximity events is sufficient, and data relating to users’ movement and location should not be collected (Ingram 2020). The thought may be: all we need to know is whether two individuals came into close enough contact for viral transmission to have occurred; we don’t need to know where or when this contact occurred, and there is no need to collect and store users’ location data.

   **Response:** This conclusion might be too hasty. As discussed above, there is potential (though unproven) benefit to providing public health authorities with location data. Location data could help jog people’s memories about where they’ve been, provide more context for understanding the nature of “proximity events” captured by the DCTT, and allow public health authorities to quickly define a category of individuals who may be at risk. Collecting location data from cases is what public health authorities do on a regular basis, following best practices for manual contact tracing.

   In addition, many people’s location data are currently gathered by apps on their phones and used for various purposes, such as to provide more accurate navigation, to offer entertainment, or to improve services. Many are willing to accept these capabilities because they provide some value in return. Why not allow DCTT to also collect these data so that the data are available for users to share with public health officials, who can then do their work more effectively and refine their understanding of how the disease transmits? If many are willing to have these data used to find a better route home, why not let individuals share these data to support the effort to save lives?
4. Proponents may hold the view that minimal systems pose little or no threat to individual autonomy, whereas systems that collect identifiable data and integrate public health do pose a threat to individual autonomy. For example, they may worry that use of DCTT could be mandated and not a voluntary choice, and in this circumstance mandatory use of minimal DCTT would be less intrusive, risky, and privacy violating. Another worry might be that it’s theoretically possible that DCTT could share individuals’ data with public health authorities without users’ full understanding; if the technology does not even gather identifiable data, then it’s not possible for these data to be shared without the individual’s consent.

Response: We discuss the importance of appropriately designed disclosures and consent below, as well as the high bar that would need to be met to ethically justify mandatory use. At this time, mandated use of DCTT by states or institutions is not justifiable, given uncertainty about potential harms and benefits. Users should have a meaningful opportunity to review and understand information about the specific technology and its uses and to consent. Assuming that individuals are not required to use DCTT and that they provide consent to using it, designing DCTT to make data collection and sharing possible is the design choice that maximizes individual autonomy, because it provides individuals with options they may value.

Individuals may wish to share their data with public health authorities for both self-interested and altruistic reasons. For example, someone who has tested positive for SARS-CoV-2 and enters this test result into an app may wish to be connected to public health authorities in order to be provided with needed information, resources, and support. She may wish for public health authorities to be provided with her phone number in case they need to reach her to provide additional information. Further, someone who has been alerted by an app that he had a “proximity event” with a person who has tested positive for SARS-CoV-2 may wish he had location data to share with public health authorities in order to help ascertain whether this event is a cause for concern or whether it is likely a false positive (e.g., he and the COV+ person were sepa-
rated by a wall). Someone who tests positive for the virus may also wish to share their location history with public health authorities in order to be as helpful as possible to the overall public health response by facilitating de-identified aggregate analyses that identify locations of higher transmission or contribute to refining overall understanding of the disease and pandemic.

5. **Concerns about “surveillance creep” and the long-term downstream effects of digital contact tracing system may also motivate embrace of minimal DCTT.**

Digital contact tracing technology that collects identifiers and location data and has the capacity to share them with public health authorities may represent a massive and concerning increase in government surveillance of the public. It might be feared that the use of this surveillance capacity in the COVID-19 response sets an unwelcome precedent for future use in other contexts. Designing DCTT as minimal systems may be a way to minimize the risk of surveillance creep and to minimize the harms associated with potential future uses of the technology.

**Response:** Surveillance creep is a serious concern. To guard against surveillance creep, 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. In the face of these concerns, it is important to emphasize that widespread use of DCTT in the COVID-19 response is justified by the exceptional circumstances of the current pandemic, and their use in this context does not imply that future public health use is ethically appropriate without significant public debate (e.g., use in seasonal flu surveillance efforts). Future use will require independent justification. Use of DCTT in other contexts (e.g., law enforcement or immigration enforcement) is also presumptively unethical.

All in all, the arguments that DCTT should be designed as a minimal system are not convincing. Rather, DCTT should be developed through a “values in design” approach, with a core set of features that protect pri-
vacy, with enough flexibility to be used differently depending upon local conditions, evolving evidence, and individual preferences. What kind of digital contact tracing system will strike the right balance between public health goals and other considerations will depend upon circumstances. For example, whether it is even beneficial to provide public health authorities with volumes of data about potential contacts of COV+ people will depend, in part, upon whether they have the capacity to make good use of those data. This will vary from location to location and will change over time.

**Recommendations**

- Technology companies should not alone control the terms, conditions, or capabilities of DCTT, nor should they presume to know what may be 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 rather it 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 and as it is shown to be critical to achieving public health goals.
Policy Positions to Advance Widespread Use of Digital Contact Tracing Technologies

The public health value of a DCTT depends in part on the number of people who use it. This section concerns broad public policy positions that relate to the widespread adoption of DCTT. What are ethical means of encouraging or securing widespread adoption of DCTT systems? Under what circumstances would it be ethical to mandate their use or incentivize their use? What enforcement challenges exist?

**Mandating Use**

Digital contact tracing has occurred without the public’s explicit voluntary agreement in some countries such as China and Israel. In others, use has been voluntary (Valentino-DeVries, Singer, and Krolik 2020). For example, Singapore adopted an app that the public could use on a voluntary basis, and approximately 20% of the population has downloaded and used it. Norway has recently launched a contact tracing app that was downloaded by roughly 30% of the population in the first week that it was made available. In the United States, many advocates and researchers have argued that use of digital contact tracing tools must be fully voluntary; this is the dominant perspective.

There are numerous ways that DCTT could be put into use without user choice. For example, as has been done in Israel, location data from mobile phones could be collected and used by the government without users’ consent. Use of an app could be formally mandated as a precondition for returning to work or school, or even further, to control entry into a facility or onto 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 contend that mandatory use of digital contact tracing tools could be ethical and may even be ethically required. Mandating use of digital contact tracing tools could, in theory, vastly increase the effectiveness of digital contact tracing systems, and thus may save more lives and allow states to lift lockdowns sooner or avoid reimposing lockdowns in the future. Canca (2020) argues that use of privacy-by-design digital contact
tracing tools should be mandatory because the use of these tools will be nearly harmless if there are sufficient privacy protections. In addition, mandatory use of DCTT that embraces these principles is significantly less intrusive at the individual level than manual contact tracing, which involves the collection of personally identifying and potentially sensitive data. In this light, it could be argued that such mandates are actually preferable from the perspective of both public health and individual liberty, insofar as they reduce the likelihood of “stay at home” orders, which are a severe limitation of individual liberty.

Nevertheless, mandated use of DCTT systems faces considerable obstacles. For example, people may not adhere to the mandate by simply leaving their phone at home, thus preventing their activities from being tracked. Even more harmful would be if people react to a mandate and a perceived violation of liberty and privacy by employing location and Bluetooth spoofing software to shield their real contacts behind a screen of misinformation. The introduction of this misinformation into a contact tracing effort might severely undermine its effectiveness. The possibility of nonadherence also raises the issue of enforcement: would high rates of nonadherence be permitted, or would enforcement be attempted (if even possible)? 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, the entity instituting the mandate, and potentially the larger public health response (Bernstein et al. 2019).

Mandatory DCTT could also be used to enforce quarantine restrictions and stay-at-home orders for those who are COV+ or are determined to be at heightened risk. The use of DCTT in enforcement activities raises a number of ethical (and legal) issues that are beyond the scope of the present analysis. In particular, individuals have a heightened interest in personal privacy if their data can be used to restrict their freedom of movement and other civil liberties. At a minimum, stringent procedural protections would be required to ensure that the data collection is fair and unbiased and that DCTT users are provided with adequate information, in advance, about how their data may be used.

Mandatory use policies for DCTT must therefore convincingly address a number of questions, including:
• Is the technology designed to meet an important and unmet public health need?
• Is there sufficient evidence to suggest that the technology will be effective at serving its purpose?
• Is the outbreak characterized by sufficiently severe morbidity and mortality and a high rate of disease transmission?
• Are there other less autonomy-restricting or less risky alternatives to widespread mandatory use of DCTT?
• Is it possible and likely that a sufficient number of individuals will comply with a mandate?
• Can inequities in the burdens and benefits of the mandate be sufficiently addressed through social protections and countermeasures?
• Can enforcement and enforcement discretion be implemented in a manner that is consonant with fundamental rights?
• Will those subject to the mandate interact closely with a population that is at high risk of morbidity or mortality if they contract the virus?
• Is it possible to mandate use and remain consistent with important ethical and legal principles?

These questions would need to be satisfactorily addressed and explicitly documented by any decision maker considering mandatory use, including government officials, institutional leaders, and employers. 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. If use of a DCTT is a condition for returning to work or school in person, those who refuse or are unable to use DCTT should not lose their jobs or positions as a result, and adequate support should be in place for people who are asked to self-quarantine.

Finally, it is important to distinguish a mandate from a “pushed” program installation or a default setting in an application which can be modified by users. A mandate relates to a policy of required use, whereas the pushed programs or default settings relate to the chosen architecture for download and operation of the application.
Perhaps the most effective way to generate widespread adoption of DCTT in the United States is to offer incentives to individuals who choose to adopt and who properly utilize the preferred DCTT approach in a voluntary system. External incentives may help “nudge” populations toward desired adoption targets. Given the importance of widespread use of DCTT, modest incentives ought to be considered for DCTT in the US if and when there is sufficient evidence of the technology’s utility. Note that in other contexts, studies have shown that the provision of some incentive leads to an increase in adoption or utilization of public health programs (Singer and Ye 2013; Lee et al. 2014). Moreover, even a relatively small incentive can achieve much greater rates of adoption, with some studies demonstrating that the incremental adoption gain decreases as the incentive gets larger (Thornton 2008; Gibson et al. 2019).

In the context of COVID-19, incentives that might be both effective and ethically acceptable could include a relatively small monetary token, free or discounted mobile phone service for a period of time, or credit to be used by means of a mobile phone.

Not all incentives are ethically appropriate. For example, making access to lifesaving health care contingent on using a DCTT or making valuable disease information available only to DCTT users would not be ethically appropriate. In addition, incentives cannot be used to overcome otherwise ethically unjustifiable technology design: for example, they should not be used as an offset for providing personally identifiable health information to other users.

Importantly, incentivization schemes must be kept distinct from mandates, as the latter require greater ethical justification. To offer an incentive is to offer something of actual value to individual participants over and above what they are reasonably entitled to at baseline. For example, making a return to work contingent on using DCTT is not offering an incentive but instead imposing a mandate, and it would have to be justified as a mandate.

In the context of COVID-19, it is also necessary to recognize that there is an *inherent* “incentive” behind the technology—that is, the promise of more lives saved, faster pandemic recovery, and the reduction or elimination of blanket physical distancing. Effective public communica-
tion of these goals, if and when there is sufficient confidence in the technology, is important.

**Encouraging Use**

Another important approach to increasing use of DCTT in the United States is for trusted leaders to encourage their use. Community leaders, public figures, health care professionals, and other respected individuals who have the public’s trust and goodwill could be enlisted to communicate with the public about DCTT and encourage its use, drawing on notions such as communal responsibility, solidarity, and so on. These encouragements could be combined with other approaches (e.g., small incentives) to optimize reach while continuing to respect individual choice.

**Recommendations**

- 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.

- 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 (i.e., they should not incentivize downloading an app but then leaving one’s phone at home).

- 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.

**Disclosure and Authorization/Consent**

In deciding whether to use DCTT *voluntarily*, individuals must be sufficiently informed, both through broad coordinated public engagement campaigns and individual-level disclosures, and there must be a meaningful mechanism for users to consent. It is important to recognize that while
informed consent—which is characterized by detailed consent forms and requires a witnessed signature—is the standard for most research and clinical care encounters (Faden and Beauchamp 1986), it is not typically the standard for public health disease surveillance. In the public health context, other relevant protections (such as ethics training for public health professionals, and strict data handling and confidentiality requirements) are in place and there is a strong public health interest in collecting the relevant data. A more limited role for consent has been recommended for public health surveillance based on a reciprocal obligation of members of society to contribute to a “common good” and, particularly in the context of a pandemic, practical considerations such as time constraints and exigencies such as increasing morbidity and mortality (WHO 2017).*

Under current circumstances, given that (1) many individuals have time and capacity to consent, (2) DCTT is being considered as part of plans for longer-term restabilization, (3) DCTT is not a familiar part of our public lexicon, (4) remote consent disclosure and authorization can be easily embedded in DCTT systems (Moore et al. 2017), and (5) there are justifiable public deficits in trust with respect to various government and corporate actors handling potentially personal digital information, a strong ethical case can be made for requiring a carefully crafted version of what is sometimes referred to as simple consent. Simple consent consists of basic disclosure and voluntary agreement or authorization (Ali et al. 2017). Three questions then arise.

1. **What information should be disclosed to potential users of DCTT?**

   • Information disclosed might include:
     
     ° Entity responsible for the technology
     ° Its purpose
     ° How it works (in lay terms)

---

* Some participatory disease surveillance systems (e.g., Flu Near You) have received formal “waivers” of consent requirements from institutional review boards (IRBs) in the US. As they undergo development, these digital surveillance systems often straddle a line between public health surveillance and research, hence the frequent need or desire to obtain ethical review by an IRB (Ali et al. 2019).
• What users need to do
• Any user options, e.g.,
  ▪ Sharing geolocation data with public health authorities when that would facilitate a defined public health goal
  ▪ Sharing de-identified metadata with technology developers (for system enhancement)
• User rights
• How data will be handled
  ▪ What data are collected
  ▪ What data are shared (and how and with whom)
  ▪ Purposes for which data can be used and not used
  ▪ How data are secured and protected
  ▪ Whether and what data will be retained (or will be deletable)
• Potential benefits and any known risks
• How to obtain answers to questions about the technology and public health response

2. How should this information be presented?

Information should be presented leveraging eConsent models that are more accessible than long “clickwrap” disclosures typical of mobile apps (Iwaya et al. 2019). For example, a simple open-source smartphone consent module that has been developed by Sage Bionetworks for research uses could be adapted to the public health surveillance context and to DCTT (Doerr, Suver, and Wilbanks 2016).

• Formatting recommendations include (cf. Doerr et al. 2016):
  ▪ simple and straightforward information
  ▪ deliberately organized content
  ▪ multimodal learning (e.g., visual, audio, written)
  ▪ accessibility for disabled users
3. How should users signal that they agree to the details specified in disclosures?

**Opt-in Models**

Opt-in models are those that, through an affirmative act such as clicking a button, users would indicate their intention to use a DCTT. This approach is consistent with other app downloads, where app details and privacy policies are made available through a download page and users are required to affirmatively click a button to install an app. Once installed, some apps further alert users to particular ways in which phone capabilities or data will be used, with some permitting selective toggling (opting-in or opting-out) of certain features. With DCTT apps, in addition to disclosures provided on a download page, the user could be guided through a simple interactive module embedded in the app (such as is described above) in order to increase the chance of meaningful exposure to important information about the technology and how data will be handled. At that point, any user options, such as those itemized above, could be described and choices made.

**Opt-out Models**

There are at least two different ways in which the term “opt-out” has been used in this context. The conventional use of the term “opt-out” is characterized by an act which signals an individual’s intention to decline something that would have otherwise occurred without intervention. A few others have used the term to refer to “revocation of consent,” for example, the United States COVID-19 Consumer Data Protection Act of 2020 Senate bill (S.3663) would establish a default opt-in position—
requiring “affirmative express consent” for collection and use of proximity and other related data—and refers to individuals having a right to later revoke their consent through an “opt-out.” The latter use of the term is not our focus here.

Given this, a DCTT app that is voluntarily downloaded through an affirmative act would be difficult to characterize as an opt-out approach. This leaves more passive surveillance systems that rely on automatic installation of self-activating technology onto users phones. There are a range of views among the authors of this report about the value of an opt-out approach for DCTT, with some arguing for an opt-out approach on grounds that it might increase coverage and would be ethically acceptable if accompanied by similar disclosures as above to ensure users are aware of the technology and data uses (Mello and Wang 2020). This approach would present users with a mechanism to opt-out if they wish, which should be reasonably easy to effectuate. Under these circumstances, as noted above, an “opt-out” would not be synonymous with mandating use of the technology.

Others among the authors argue that there is reason to believe that opt-in approaches may be able to sufficiently achieve desirable levels of utilization relative to opt-out approaches. Unfortunately, data related to opt-in versus opt-out models of DCTT are very limited. One recent survey (Altmann et al. 2020) found that across five countries (UK, Germany, France, Italy, US), slightly more people reportedly would download an app under an opt-in system (74.8%) than would keep an app on their phone under an opt-out system (67.7%). Moreover, when US respondents were directly asked which approach they would prefer, 60% indicated a preference for opt-in. This remained true across various demographic variables—gender, region, political affiliation, lockdown status, and other characteristics. Whether actual behaviors would align with anticipated behaviors in the context of DCTT remains an unanswered question that should be carefully studied under real-world conditions. There are a range of important empirical questions regarding how much and what kind of impact (positive or negative) various types of defaults might generate for public health and for different mobile phone user groups, including vulnerable and marginalized users.

Opt-out models for app authorization may encounter greater legal
and political challenges, especially if the COVID-19 Consumer Data Protection Act of 2020 (S.3663), the competing Public Health Emergency Privacy Act (S.3749), or another similar bill is enacted in the United States. Both of these standing bills require affirmative opt-in consent. Opt-out approaches also risk negative reactions from some mobile phone users, a small number of whom may go so far as to intentionally interfere with data because of the perceived intrusiveness of an automatically installed tracking platform (Dixit 2020).

Given these considerations and the apparent willingness of a large portion of the population to opt-in to use DCTT, 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. Opt-out approaches should not be precluded.

Recommendations

- 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.
Digital contact tracing technologies 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. For example, communities with lower rates of technology and data access may benefit less from DCTT. Special attention must be paid to communities that experience preexisting health disparities and to those that are being hardest hit by the pandemic.

**Digital Disparities**

In the United States, February 2019 data indicate that approximately 80% of the population are smartphone users (Pew Research Center 2020), though rates of mobile phone use are significantly lower among people over age 65 (53%), people with any disability (58%; 2016 data) (Anderson and Perrin 2017), people with less than a high school education (66%), people who earn less than $30,000 per year (71%), and people who live in rural areas (71%). As a result, these populations and communities may use DCTT in lower numbers, thereby lessening the effectiveness of DCTT and the likelihood of benefit for these populations from such systems. Moreover, it has been reported that many older and less costly smartphones (roughly estimated at 10%–20% of smartphones in the US) lack important capabilities required for the leading Apple/Google platform to work (Bradshaw 2020). This is of special concern because some of the above groups that are less likely to own smartphones in general are also less likely to own newer smartphones with the needed capabilities. Some within the above groups (e.g., people who are older and people identified as Hispanic, African American, or American Indian) are also disproportionately experiencing morbidity and mortality from COVID-19 (CDC 2020h).

One may argue that by using DCTT, human and financial resources that would otherwise be spent on manual contact tracing will be preserved, and these resources can then be redirected to better meet the needs of those who are not otherwise being effectively served by the technology because of disparities or for other reasons. This argument has intuitive
appeal and should be taken seriously; however, it is unsettled whether DCTT will contribute sufficient efficiencies to the overall public health response to make it possible, financially and logistically, for manual services to be allocated in greater proportion to those who are unable to benefit from DCTT. It is entirely possible that, at least in the short-term, DCTT may introduce new inefficiencies due to unintended consequences or the need for public health officials to follow up many more contacts. One possible mitigation to the challenge of digital disparity—though it does not solve the underlying challenge of ensuring net efficiency across systems—might be to provide mobile phones or other devices and data packages to those who would otherwise be left out.

Disparate Risk of Harm from Surveillance and Data Gathering

Ensuring wide digital coverage does not, however, resolve other equity concerns. It is important to consider that some populations may experience greater harm, and 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 (CSM 2017; Pew Research Center 2017; Rodrigues et al. 2018; Auxier et al. 2019). Any data gathered by DCTT should be used solely for public health purposes. Efforts should be made to assure members of these and other communities that their data will not be misused or made available to those outside of a public health context. In addition, if DCTT are used in the current pandemic, this should be with the understanding that future use of DCTT in other contexts (e.g., law enforcement or immigration enforcement) is presumptively unethical.

Some preliminary polling related specifically to DCTT emphasizes the complexity of the challenges faced and the need for deeper public engagement (Anderson and Auxier 2020). The polling results suggest that people who identify as African American or Hispanic are more likely than people who identify as White to consider government tracking of mobile phones as acceptable. These findings, like many others, are difficult to interpret given background political polarization on the issue. More direct engagement is required to better understand how different communities comprehend and experience DCTT and other forms of surveillance.
Discrimination and Stigma

Stigma may result from an individual being identified as COV+, or a neighborhood or establishment becoming identified as a “hotspot” as a result of numerous COV+ people living in that area or having visited that establishment. In particular, certain groups may suffer more as a result of being associated with COVID-19, such as the well-documented blame that has been directed toward Chinese people (and broadly East Asian communities) or the communities that are disproportionately likely to contract the illness (Devakumar et al., 2020). When identifiable location data are made public, as has been the case in South Korea, personal and private information were revealed. Furthermore, businesses in South Korea that were identified as having patrons who tested positive for COVID-19 have suffered economic losses and stigma (N. Kim, 2020).

To avoid the stigma and potential discrimination that can result from being identified as COV+, DCTT must never make data publicly available that could be used to identify persons who have tested positive. Safeguards must be in place to ensure that any identifiable data that may be gathered for public health purposes are protected. If DCTT data are used to provide heat maps to the public of locations that COV+ individuals frequently visit so as to provide representations of geographic risk or for other reasons, it is essential that care be taken to avoid unfairly distributing further economic burdens or other stigmatizing and discriminatory outcomes.

Recommendations

- A commitment to equity means a commitment to ensuring that the benefits and burdens of DCTT are distributed fairly. Public engagement is an important tool for assessing impact and to rectify inequities.

- 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 iden-
tify 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 being identified as a hotspot.

**Instituting Transparent Governance and Oversight**

DCTT must be developed with an eye toward both present and future implications. Transparent and publicly trustworthy management, governance, and oversight of DCTT technology and data is both a near- and long-term necessity. We face significant uncertainties. DCTT technologies are rapidly developing. Their risks, capabilities, effectiveness, and downstream implications are not yet well understood.

**Concerns about “Surveillance Creep”**

Significant concerns have been expressed by privacy advocates (Guargiglia 2020) and in the popular press (Giglio 2020) about what is known as “surveillance creep.” Their worry is that state and 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 should be guarded against. Only those data that are necessary and relevant for the public health purposes at hand should be collected and used, and data should be kept only for the period of time needed for those public health purposes. Data should be used only for public health purposes.

Any use of DCTT during the current pandemic would be justified by the circumstances of this pandemic, and its use in this context does not set a precedent for future public health use (e.g., use in seasonal flu surveillance efforts). Future use will require independent justification. Use of DCTT in the future in other contexts (e.g., law enforcement or immigration enforcement) is presumptively unethical.

Broadly speaking, efforts should be made to generate public aware-
ness and consensus that use of DCTT in COVID-19 efforts does not imply that future use is justifiable. However, generating this public awareness may be particularly challenging given the complexity of the informational environment, where public debate ranges from legitimate concerns about surveillance creep to conspiracy theories regarding the origins of the COVID-19 pandemic (Muller 2020). This means authorities bear special obligations to be clear on how they plan to use the technologies, what oversight mechanisms will be employed to address potential abuse, and how they intend to publicize the conditions under which programs will be terminated, making sure they are followed.

**Oversight and Ethical Review**

We are rapidly gaining knowledge about SARS-CoV-2 and COVID-19, but we 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, and associations (Reston, Sgueglia, and Mossburg 2020). 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.

To address the range of ethics-related concerns about the design and use of DCTT, digital surveillance oversight committees should be established, perhaps at a state level and with a platform for national coordination. These committees can provide ethical and regulatory review prior to and concurrent with widespread use of DCTT. These committees should be composed of a diverse group of experts capable of evaluating 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. What kind of precedent might use of these technologies during the current pandemic set for future use capabilities in other infectious disease outbreaks or in other social contexts (e.g., law enforcement)? 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 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.

**Recommendations**

- 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 collection, 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.