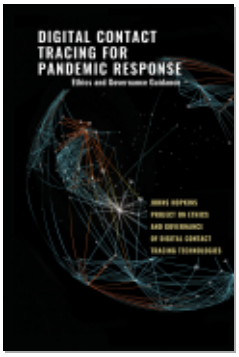
Digital Contact Tracing for Pandemic Response

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.

FOUR

Legal Considerations

The implementation of digital contact tracing technology (DCTT) is likely to implicate a number of US laws at both the federal and state levels. This section focuses primarily on federal laws, as these laws apply nationwide and generally preempt conflicting state laws. A comprehensive assessment of the legality of any particular DCTT program would require case-specific analysis and attention to relevant state laws, including any that specifically address DCTT, which may soon exist in one or more states. The analysis here is limited to the United States; foreign and international laws will not be addressed.

Many of the laws discussed in this section are privacy laws designed to protect individuals from the harms that may result from the unauthorized or improper use of their personally identifiable information (PII). Under these laws, legal concerns will generally be minimized if privacy protections are built directly into the DCTT technology (e.g., "privacy by design"). As a general principle, DCTT should be designed to collect and store only as much PII as is necessary to achieve the public health purpose. Collecting only proximity data, for example, is likely to raise fewer legal concerns than collecting both proximity data and geolocation data. Likewise, creating aggregated, anonymized, or de-identified data will raise fewer legal concerns than using and disclosing PII.

As we have argued elsewhere in this guidance document, however, the public health and societal crisis caused by COVID-19 may justify

greater encroachments on individual privacy than would otherwise be permissible. Regardless of the type of data collected, privacy concerns will be reduced if users are afforded the right to choose whether their PII is collected and how it is used and disclosed. As such, DCTT should generally secure meaningful user consent before collecting PII, a process which typically requires both disclosure of relevant information and agreement on the part of the user.

Privacy concerns will also be reduced if the use of PII is strictly limited to tracking and limiting the spread of SARS-CoV-2. The use of DCTT data for other purposes—such as commercial or law enforcement purposes—would raise additional legal and ethical concerns. In addition, DCTT developers may be required to implement governance policies that ensure the secure storage of PII, limit data retention periods, require transparency about data sharing, and maintain records of responses to data requests from government authorities.

In short, the legality of a DCTT program under current United States law will depend on a number of factors, including what type of data is collected; how the data are used and who may access them; how user consent is obtained; whether the entity collecting and using the data is the government or a private corporation; the context in which data are collected (e.g., employment, education, or commercial); and which states have jurisdiction over the program.

Privacy law in the United States, unlike in other jurisdictions such as the European Union (EU) and Australia, is generally sector-specific and limited in scope. The result is a patchwork of protections that differ significantly depending on the entity that collects the data and the type of data collected. For example, under current law, telecommunication carriers are governed by different privacy rules than mobile broadband providers. Given the complexity of existing federal privacy law, we believe that it would be beneficial for the US Congress to enact new privacy legislation that is specifically tailored to the use of DCTT in response to COVID-19. Congress appears poised at least to debate such legislation: a pair of bills recently introduced in the Senate and one in the House of Representatives would significantly restrict the collection of PII by digital devices for COVID-tracing purposes. S.3663, S.3749, H.R. 6866, 116th Cong. (2020).

Telecommunications

A DCTT provider that collects data from a user's mobile phone may be subject to the privacy rules governing telecommunication carriers, which are enforced by the Federal Communications Commission (FCC). The data protected under these rules are limited, however, to certain types of PII, termed "customer proprietary network information" (CPNI). Moreover, the rules generally apply only to telecommunications carriers and interconnected VoIP (Voice over Internet Protocol) providers.

In particular, under section 222 of the Communications Act of 1934, 47 U.S.C. § 222, and the implementing regulations of the Federal Communications Commission (FCC), telecommunications carriers and VoIP providers must establish and maintain systems designed to ensure that they adequately protect their subscribers' CPNI, and they are generally restricted from using or disclosing CPNI without the customer's consent (unless the use of disclosure is needed to provide the services subscribed to by the customer). If customer consent is sought to use or disclose CPNI, individual notice must be provided to the customer, and such notice must provide sufficient information to enable the customer to make an informed decision as to whether to permit the requested use or disclosure.

CPNI is individually identifiable information that carriers and providers have collected about their customers, including phone numbers called and the frequency, duration, and timing of such calls. Of most relevance to DCTT, a recent FCC Notice of Apparent Liability asserted that user geolocation data collected by mobile phone network carriers qualify as CPNI under § 222 and related rules. 35 FCC Rcd 1785 (2) (2020). Pursuant to this notice, the FCC fined T-Mobile for selling to third parties location data that were derived from the communication between the mobile phones of T-Mobile's customers and nearby network signal towers. (The FCC also levied fines against AT&T, Verizon, and Sprint on the same grounds (Valentino-DeVries 2020).) While the FCC has made its position clear that geolocation data are CPNI, courts have yet to weigh in on the matter.

Even if geolocation data are CPNI, however, the FCC can enforce § 222 of the Communications Act only against telecom carriers and VoIP

providers, not against cable broadband and mobile broadband internet providers. 47 U.S.C. § 53(44), 47 C.F.R. § 9.3. In 2018, the FCC promulgated a regulation stating that, contrary to its prior position, its § 222 authority does not extend to cable broadband and mobile broadband internet providers. Restoring Internet Freedom, 83 Fed. Reg. 7852 (Feb. 2, 2020) (to be codified at 47 C.F.R. pts. 1, 8, and 20). This regulatory shift was subsequently upheld by the DC Circuit, *Mozilla Corporation v. Federal Communications Commission*, 940 F.3d 1 (2019).

In addition to § 222, the FCC has authority to regulate "common carriers"—including both telecommunication carriers and broadband internet providers—under § 201(b) of the Communications Act. In the past, the FCC has interpreted § 201(b) to protect against "unjust and unreasonable" privacy and data security practices with respect to customers' personal information beyond CPNI. In 2016, the FCC promulgated a regulation asserting its authority under this interpretation. However, Congress overturned this regulation pursuant to the Congressional Review Act in 2017. S.J. Res. 34, 115th Cong. (2017). At present, the extent of the FCC's authority under § 201(b) remains unsettled (Mulligan and Linebaugh 2019).

Consumer Protection

The collection, storage, release, and transmission of digital user data, including proximity contacts, is more generally governed by the Federal Trade Commission (FTC). The FTC is an independent US law enforcement agency tasked with protecting consumers and promoting competition across broad sectors of the economy (FTC 2020). The FTC's primary legal authority with respect to consumer protection comes from Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). Note that the FTC and FCC have some overlapping authority to protect consumer privacy in the context of telecommunications (FCC and FTC 2017).

The FTC has interpreted Section 5 to require companies to be transparent and accurate about their collection of PII from consumers. A company may be found to have engaged in a deceptive practice if it fails to disclose that it is collecting user data or fails to disclose that it is sharing these data with third parties and to provide a general description of these third parties. The FTC has used its authority under Section 5 numerous

times to discipline companies that purport in published privacy policies or other notices to provide protection for the privacy and/or security of personal information, yet fail to do so in practice. For example, the FTC may find it both "unfair" and "deceptive" for a mobile app privacy policy to state that the app never discloses location information to third parties, when in fact the app shares that information with the app developer's service provider, which in turn uses it to provide analytical data to the app developer that are used to create targeted advertising.

The FTC does not use its Section 5 authority other than to protect consumers and generally does not consider "de-identified" user data, which are data that are not "reasonably linkable" to a consumer, to be a subject for consumer protection. In general, data collected are not "reasonably linkable" so long as the company collecting it "(1) takes reasonable measures to ensure that the data are de-identified; (2) publicly commits not to try to reidentify the data; and (3) contractually prohibits downstream recipients from trying to reidentify the data" (FTC 2012).

Many states have laws that are similar to Section 5, prohibiting unfair and deceptive acts and practices. Both Section 5 and these similar state laws can be violated not only by misrepresentations (affirmative deception) but also by material omissions. Thus, a failure to inform an app user of the app's collection of tracking data and the planned use and disclosure of those data could constitute a violation of these laws. Companies providing DCTT apps should make sure that all such information is disclosed in the apps' terms of use to which users must affirmatively agree.

Children's Online Privacy

Children who use DCTT may be protected by additional privacy protections. In particular, collection of digital PII from children under the age of 13 is strictly regulated under the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§ 6501–6505). Under COPPA, PII includes "first and last name[;] a persistent identifier that can be used to recognize a user over time and across different . . . online services[;] and geolocation information sufficient to identify street name and name of a city or town[.]" COPPA prohibits a website or online service from collecting personal information (including location information) from children under age 13 without obtaining verifiable parental consent. Note that there may be an

exception to this requirement for an "investigation on a matter related to public safety." 16 CFR § 312.5(c)(6)(iv).

Electronic Surveillance

In addition to misuse of user data by DCTT providers, another privacy concern is that a third party may be able to access sensitive PII that is collected and stored by a DCTT system without the user's knowledge and consent. There are a number of federal criminal laws, however, that would likely prohibit such unauthorized access to PII.

In particular, the Electronic Communications Privacy Act of 1986 (ECPA)—which includes the Wiretap Act (18 U.S.C. §§ 2510–2522), the Stored Communications Act (18 U.S.C. §§ 2701–2711), and the Pen Register Act (18 U.S.C. §§ 3121–3127)—makes it a crime to access electronic communications without authorization. Individuals who violate the ECPA face up to five years in prison and fines up to $250,000. Victims are also entitled to bring civil suits and recover actual damages, in addition to punitive damages and attorney's fees, for violations.

Generally, the access restrictions in the ECPA apply unless consent is given or if access is authorized by statute for law enforcement purposes. For example, an employer is generally forbidden from accessing an employee's private emails. However, if consent is given in the form of an employment contract that explicitly authorizes the employer to access emails, it may be lawful under the ECPA for the employer to access such information. Along the same lines, the ECPA would likely prohibit an employer from accessing contact tracing data on an employee's phone without the employee's consent. However, the ECPA would likely not prohibit duly authorized government public health officials from accessing contact tracing data without consent.

As its name suggests, the Stored Communications Act (SCA) regulates access to communications at rest, that is, not in transit. The SCA makes it unlawful to intentionally access a facility in which electronic communication services are provided and to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such a system. As such, the SCA would likely apply only to centralized collection of contact tracing data.

The Pen Register Act covers any "signaling information" exchanged in a communication, such as phone numbers. The statute does not reach

the content of such communications, however. An expansive interpretation of the Pen Register Act would cover Bluetooth "handshakes," as they are merely signaling information between devices, which do not carry content. See *United States v. Forrester,* 512 F.3d 500 (9th Cir. 2007) (finding that email headers and IP addresses are akin to pen registers and have no Fourth Amendment protection). Unlike the SCA, there is no statutory exclusionary rule that applies when the government illegally uses a pen register / trap and trace device. Additionally, there is no private cause of action against the government for violations of the Pen Register Act.

State Data Privacy Laws

States have a variety of privacy laws and are increasingly seeking to regulate the online collection of personal information and the use and disclosure of such information. To date, most of these laws focus more on transparency and protection from unauthorized access than on restricted collection and use (except with respect to biometric information), seeking to ensure that individuals who use websites or online services such as mobile applications do so on an informed basis with respect to the privacy provided by those sites and services. Two examples of such state laws are the California Online Privacy Protection Act (CalOPPA) and the California Consumer Privacy Act (CCPA). Both laws require notice to individuals who use websites or online services such as mobile applications, in order to ensure that users are informed about the privacy of personal information collected by those sites and services. (The CCPA also applies to data collection off-line.) Both laws treat IP addresses and location data as types of potentially identifiable personal data, and so would very likely apply to DCTT apps used by California residents.

CalOPPA requires that the operator of any website, mobile application, or other online service ("Site") post a privacy policy on the Site disclosing certain information regarding the Site's collection, use, and disclosure of PII. CalOPPA applies to any Site that is accessible to California residents. The required disclosures are not onerous and would apply only to collection of data that are identifiable to an individual person (but, depending on who collects the data, location data together with a device identifier are identifiable to the user).

The CCPA requires that any entity qualifying as a "business" provide its "consumers"—defined as lawful residents of California—with specific

disclosures about the business's collection, use, and disclosure of personal information. Importantly, the CCPA applies only to for-profit businesses that meet certain thresholds of revenue or access to consumer information. A public health agency or a nonprofit organization would not be subject to the CCPA. Cal. Civ. Code § 1798.140(c).

The CCPA defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The statute provides a nonexclusive list of potential identifiable personal information, including "geolocation data." In accordance with the CCPA, businesses must provide consumers with a notice "at or before the point of collection" of personal information, which must describe the personal information to be collected and the purposes for collecting that information. Businesses must additionally allow consumers to request access to and request deletion of personal information. Businesses must allow for consumers to opt-out of the sale of any personal information. Developers of COVID-tracing apps would want to build in compliance with these requirements. In addition, California Civil Code § 1798.81.5(a)(1) requires companies to "maintain reasonable security procedures and practices appropriate to the nature of the information it processes."

Like privacy laws generally, the CCPA does not grant consumers rights regarding the use of de-identified information. However, the CCPA does require businesses to implement processes that prohibit re-identification of de-identified information, as well as technical safeguards to prevent inadvertent release of that information. Cal. Civ. Code § 1798.140(h).

Health Information Privacy

Many DCTT systems will be designed to collect health-related data of users, such as symptom tracking, SARS-CoV-2 test results, and prior exposure to a person who is COV+. Individuals may have additional privacy protections with respect to the use and disclosure of this health-related information.

The use and disclosure of individually identifiable health information is strictly regulated under the privacy and security rules implementing the

Health Insurance Portability and Accountability Act (HIPAA). HIPAA is limited in application, however, to health care providers and health insurance plans ("covered entities") and "business associates" of such entities. "Business associates" under HIPAA are persons who perform services for covered entities and need access to personal health information to do so.

HIPAA-covered entities must have written authorization to use or disclose identifiable health information ("protected health information," or PHI) from the individual to whom such information pertains, unless the HIPAA regulations promulgated by the US Department of Health and Human Services (HHS) provide an exception to the requirement for such individual authorization.

Among the exceptions to the individual authorization requirement is an exception for certain uses and disclosures of PHI for public health purposes. 45 CFR § 164.512(b). This exception would permit, for example, a HIPAA-covered entity to disclose the PHI of an individual who tests positive for SARS-CoV-2 to a public health authority. A "public health authority" is an agency or authority of the US government, a state, territory, a political subdivision of a state or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency, such as a contact tracer. Id. § 164.501.

Many DCTT developers are HIPAA business associates, and any use and disclosure of PHI collected through DCTT used on behalf of HIPAA-covered entities is restricted under the HIPAA privacy rules. Notably, in response to COVID-19, HHS announced that its Office for Civil Rights would exercise its enforcement discretion and would not impose penalties for violations of certain provisions of the HIPAA Privacy Rule against health care providers or their business associates for the good faith uses and disclosures of protected health information for public health and health oversight activities during the nationwide public health emergency. 85 FR 19392 (2020).

Many states also have health information privacy laws. The HIPAA privacy rule sets a "floor" of privacy protections, allowing the states to be more protective of privacy. More specifically, HIPAA preempts a state law if (but only if) the state law is "contrary" and less protective of privacy than the HIPAA privacy rule. However, if a state law is determined by the

Secretary of HSS to be necessary to serve a "compelling need related to public health, safety, or welfare," it may survive preemption even if it is less privacy-protective than HIPAA. 45 CFR § 160.203 (a)(1)(iv).

The Public Health Service Act also restricts the use of certain personally identifiable information collected by entities involved with public health activities without the individual's consent. 42 U.S.C. 242m(d).

Labor and Employment Privacy Rights

Labor and employment laws—that is, laws that govern the relationships between employers and employees—may prove relevant to DCTT, especially if employers mandate the use of DCTT or seek to collect health information regarding their employees using DCTT. Depending on the built-in privacy protections of the DCTT system, an employer may be able to access important health information from an employee's phone. As noted above, the ECPA would generally prohibit an employer from accessing this information without the employee's consent. Even with consent, however, there are limits on the collection and use of an employee's health information.

In particular, the use of DCTT may raise special concerns about employment discrimination, for example, if an employer were to fire an employee who tests positive for SARS-CoV-2 (COV+) or who has a known SARS-CoV-2 exposure. The Americans with Disabilities Act (ADA) protects disabled employees from discrimination and restricts the collection of personal health information by employers. The Equal Employment Opportunity Commission (EEOC), which is the federal agency tasked with enforcing the ADA in the employment context, would likely consider COV+ to be a "disability" under the ADA and analogous state laws prohibiting discrimination against disabled people. COV+ is likely to be a "disability," especially where the individual is symptomatic and/or experiences related health issues, or if it is later determined that testing positive for SARS-CoV-2 leads to long-term or chronic health effects. "Exposure to a COV+ person" could also be covered by those laws because a person exposed to a COV+ individual could well be perceived as being disabled by being considered likely to be infected.

The ADA generally requires that businesses make "reasonable accommodations" for persons who are disabled, which may include individuals who are COV+ or who have a preexisting disability that places them at higher risk from or may be exacerbated by COVID-19. The EEOC has published guidance on reasonable accommodations under the ADA and related laws in the context of COVID-19 (EEOC 2020). Among other things, this guidance clarifies that, consistent with the ADA, employers may take temperatures or otherwise collect health information about employees during the pandemic crisis, so long as they keep that information confidential. As of May 18, 2020, the EEOC has not provided guidance that specifically addresses the applicability of the ADA to the use of DCTT by employers.

In addition, employment laws, such as the ADA and the Family and Medical Leave Act (FMLA), and state law equivalents, generally limit disclosure of information and require employers to keep confidential any employee personal health information related to a disability or request for medical leave. Under the ADA, any information regarding the medical condition or history of an employee that an employer obtains as part of an examination or inquiry into a disability could constitute a confidential medical record that can be disclosed only to certain individuals in limited circumstances. 42 U.S.C. §§ 12112(d)(3)(B) and 12112(d)(4). The FMLA also prevents the disclosure of records related to medical histories in connection with an employee's leave request or eligibility. 29 C.F.R. § 825.500(g). The EEOC and some courts have gone further and taken the position that any information concerning an employee's medical condition is protected under the ADA or FMLA.

As discussed elsewhere in this guidance document, employers may have a good reason to employ DCTT in order to ensure workplace safety and limit the spread of SARS-CoV-2 in the community. Employers may also face legal liability if they fail to protect employees (or customers) from potential exposure or infection. In particular, employers have an obligation under the Occupational Safety and Health Act to keep the workplace safe for employees. In response to COVID-19, the Occupational Safety and Health Administration (OSHA) has developed guidance on preparing the workplace (OSHA 2020). The CDC has also prepared guidance on healthy business operations and reducing the spread

of SARS-CoV-2 in the workplace (CDC 2020c). Employers must strike an appropriate balance between avoiding employment discrimination and promoting workplace safety.

Reflecting the need for such a balance, the employee protections under the ADA and other employment laws are not absolute and are limited by, among other things, the need to protect the health and safety of other employees and the public. Protection for workplace safety and health generally will justify appropriately tailored measures, such as inquiries into an employee's personal health status or whether someone has tested positive for SARS-CoV-2, temperature checks, and removal of employees from the workplace who are experiencing symptoms or have tested positive and have not been cleared to return to work.

Note, finally, that the use of DCTT by employers should be evaluated in conjunction with the hazard pay, sick leave, and other benefits that are available to employees. Under the Families First Coronavirus Response Act, employers with more than 50 employees and fewer than 500 employees are required to provide two weeks of paid sick leave to an employee who stays home because of COVID-19. Pub. L. No. 116-127, 134 Stat. 178 (2020). This paid leave extends to those who are themselves ill, are quarantined, or are awaiting a diagnosis, as well as those who are caring for sick family members. However, reporting suggests that more than 75% of US workers will not qualify for benefits under this act (Cochrane, Miller, and Tankersley 2020).

Constitutional Privacy Rights

A DCTT program involving only private actors operating on the basis of voluntarily provided information would not present constitutional privacy issues. But any government-directed use of digital technology to support public health tracking and contact tracing involving mandatory government surveillance may potentially implicate a variety of constitutional protections. These constitutional protections apply to actions taken by any level of government in the United States. While state governments have broad policing powers in the area of public health (*Jacobson v. Massachusetts*, 197 U.S. 11 (1905)), and are generally allowed to enforce legislation not preempted by federal laws, even emergency and

health-protective laws must be consistent with the US Constitution (HHS 2019; CDC 2020f).

Fourth Amendment Search and Seizure

Many people considering whether to use a DCTT app may be concerned that government enforcement agencies would obtain tracing data and use those data to conduct criminal prosecutions or immigration proceedings. Constitutional protections, notably the Fourth Amendment's limit on warrantless searches, limit the government's use of personal data in the criminal context. However, exceptions exist, allowing law enforcement to access information even when such access would generally be prohibited. How the government accesses personal data stemming from contact tracing needs to be scrutinized, and protections will hinge on the manner of access.

In general, the Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." As originally interpreted, the Fourth Amendment was considered tied to common-law trespass. That is no longer the case. US Supreme Court precedent interprets the Fourth Amendment to protect "people, not places" and extends to the protection of certain expectations of privacy, such as location information, as long as such expectations are reasonable. *Katz v. United State*s, 389 U.S. 347, 351 (1967). A warrantless government search is unconstitutional when the information sought is private and such expectation of privacy is "one that society is prepared to recognize as reasonable." *Smith v. Maryland,* 442 U.S. 735, 743–44 (1979).

The constitutionality of a search will revolve around the following analysis: whether the digital program either violates an individual's "reasonable expectation of privacy" (likely triggered by programs collecting large amounts of location and/or health data) or involves a government "trespass" (likely triggered by required app downloads). *Katz v. United States*, 389 U.S. 347 (1967), *United States v. Jones*, 565 U.S. 400 (2012).

Courts will most likely weigh the intrusiveness of the measures taken in implementing a search standard against the severity of the situation, governmental and individual interests, and accountability measures and safeguards built into the system.

Voluntary sharing by individuals of their information with other par-

ties, including the government, would mean that there was no reasonable expectation of privacy and would not raise the issues elaborated above. It is worth noting that consent may not be considered voluntary if coerced or conditioned, especially with regard to public employees or students of public institutions.

Third-Party Doctrine

Some legal doctrines allow for the government's acquisition of otherwise private information consistent with Fourth Amendment privacy protections. The third-party doctrine, for example, provides that individuals have no reasonable expectation of privacy in information voluntarily shared with others, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. *Smith v. Maryland*, 442 U.S. 735 (1979), *United States v. Miller*, 425 U.S. 435 (1976). This applies to information provided by third parties (mobile carriers, internet service providers, medical tracking device manufacturers, etc.) to the government under order or request, even when the third party's end-user agreements or privacy policies create an expectation of privacy.

The Supreme Court has narrowed the applicability of the third-party doctrine to exclude use and disclosure of "historical" cell-site location information (CSLI) data. For example, in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Court reasoned that the third-party doctrine does not justify use and disclosure of historical CSLI because an individual does not provide that information voluntarily. Rather, that information is pervasively collected by the cell phone company without any affirmative action on the part of the individual. The Court did not express a view on "real-time" CSLI—location information that live-tracks a cell phone's location—or on GPS data that may be stored in the phone itself.

The Carpenter decision builds on a line of cases related to searches of digitally stored location data. In *Riley v. California*, 134 S. Ct. 2473 (2014), the Court held that absent exigent circumstances, law enforcement must obtain a warrant to search an individual's phone. Exigent circumstances are those that require immediate action because there is a probability that evidence may be destroyed. The use of a centralized database for collection of digital contact tracing data would obviate deletion

concerns. If the data are stored locally in the phone, issues may arise as to whether law enforcement may suspect the data may be deleted following an arrest.

Similarly, in *United States v. Jones*, 132 S. Ct. 945 (2012), Justice Sonia Sotomayor authored a concurring opinion, arguing that the use of a GPS to track a defendant's whereabouts has the potential of providing the government with enough data points to create a "mosaic" of the person's life. Location data obtained through centralized location contact tracing have the potential of providing information on an individual's whereabouts beyond what's necessary for determining proximity to infected individuals. Localized data may also raise the same issues if accessed by law enforcement.

Following *Carpenter*, several courts have addressed the constitutionality of novel location tracking. In Massachusetts, for instance, a federal district court concluded that police use of a "pole camera" on a utility pole to investigate the movements of an individual constituted a search under the Fourth Amendment. *United States v. Moore-Bush*, 381 F.Supp.3d 139 (D. Mass. 2019). The court reasoned that, even in a public space, an individual still retains a reasonable expectation of privacy "in the whole of their physical movements." Citing *Carpenter* and *Jones*, the court stated that the government's unrestrained power to collect data that reveal private aspects of identity is susceptible to abuse and gives police access to a category of information that is "otherwise unknowable." Long-term monitoring of a person's movements, consequently, violates that individual's expectation of privacy. Notably, the court emphasized the capability of the camera to create a searchable digital log of the photos taken for the eight-month period during which the camera was used.

State courts have also weighed in on the issue. The Massachusetts Supreme Judicial Court found that police access to real-time location data pinpointing an individual's movement, whether from a third party or a cell-site simulator, infringes upon an individual's reasonable expectation of privacy. *Commonwealth v. Almonor*, 120 N.E.3d 1183, 1195 (Mass. 2019). The Washington Supreme Court, for its part, held that a cell phone ping used to locate the defendant's vehicle in real time is a search under the Fourth Amendment requiring a warrant absent exigent circumstances. *State v. Muhammad*, 428 P.3d 1177 (2018). And the Colo-

rado Court of Appeals held that police use of a video pole camera to continuously surveil a defendant's fenced-in backyard constitutes a search under the Fourth Amendment. *People v. Tafoya*, 2019 BL 457321, Colo. Ct. App., 17CA1243 (2019).

Application of *Carpenter* by lower courts to novel location-tracking tactics is still evolving, and it is as yet unclear how the narrower interpretation of the third-party doctrine will continue to be expanded and applied, particularly in cases of short-term monitoring of massive amounts of location and/or health data. Moreover, it is unclear whether *Carpenter* would apply to DCTT data collected by the government itself.

Special Needs Doctrine

An argument in favor of the constitutionality of government DCTT programs is that the "special needs" doctrine would apply. Under this doctrine, a warrantless search that would otherwise violate the Fourth Amendment might be permissible based on a special need relating to public health. When the search is conducted for a nontraditional law enforcement purpose, and circumstances make securing a warrant impracticable, the Supreme Court has ruled that warrantless searches may be permissible. The special needs doctrine, however, is highly controversial because it is not a consistently applied Fourth Amendment exception, so it is difficult to predict when courts would authorize nontraditional surveillance. Some factors considered by the court are (1) the balance between the intrusiveness of the government action and the anticipated public benefits, (2) the existence of legislative authorization, (3) judicial process or the ability of the subject individual to challenge the government action, (4) the scope or breadth of government action, and (5) the likelihood of the collected data being used in criminal proceedings. The Supreme Court did note in *Chandler v. Miller*, 520 U.S. 305 (1997), that a "risk to public safety [that] is substantial and real" may justify "blanket suspicionless searches calibrated to the risk," citing as examples the routine searches conducted at airports and entrances to some official buildings. (Searches within the context of immigration are further analyzed below.)

Immigration Enforcement

Exceptions apply to the constitutional requirement that a warrant accompany an unreasonable search or seizure in the immigration context.

For example, an exception to the general warrant requirement is the border search exception, which allows government officials to search and seize, without a warrant, persons and property at the border or at the functional equivalent of a border. See *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985); *United States v. Flores-Montano*, 541 U.S. 149 (2004). Federal regulation authorizes immigration officials to operate within 100 miles of any US external boundary. (See 8 CFR § 287.1, defining "reasonable distance" as "within 100 air miles from any external boundary of the United States.") A functional equivalent of a border may include any airport where international flights may be received, automobile checkpoints servicing international traffic, and vessels in territorial waters. Government officials, however, must still have "reasonable suspicion" of an immigration violation or a crime to search or seize persons or property.

In the context of digital data, Customs and Border Protection (CBP) officials may conduct either manual or forensic searches of electronic devices at the border, or its functional equivalent. A manual search is considered a routine search and may include accessing the phone and "browsing" its contents. If the electronic device is password protected, individuals must provide information for unlocking the device. Forensic searches, on the other hand, are nonroutine and involve a more invasive search of the electronic device's contents. Federal circuit courts are split on whether a CBP agent needs "reasonable suspicion" before conducting a forensic search of an electronic device. But Supreme Court precedent clearly states that suspicionless searches are not unconstitutional when public safety is considered. *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602 (1989).

A recent CBP directive provides guidance and standard operating procedures regarding forensic searches of electronic devices. CBP 3340-049A, Border Search of Elec. Devices (D.H.S. 2018). The directive states that CBP officers may detain electronic devices, or copies of the information contained within these devices, for a reasonable period time, not to exceed five days. This directive raises the concern that travelers may be required to turn over contact tracing data stored on their phone to CBP officers. Note that the directive has been challenged in federal court and is currently awaiting appeal. *Alasaad v. Nielsen*, 419 F.Supp.3d 142 (D. Mass. 2019).

Searches in Schools

Another exception to the general warrant requirement applies to searches by non-law-enforcement government officials in public schools (i.e., school officials). Within this context, school officials have broad powers to conduct searches as long as those searches are reasonable. Searches by individuals in private schools are not governed by the Fourth Amendment. State regulation of searches in private schools varies. (See US DOE 2009.)

Related Federal Privacy Statutes

Outside the Fourth Amendment context, certain laws provide protections against government collection of and access to personal data. The USA Freedom Act of 2015, for example, bans the government's bulk collection of internet metadata and telephonic records, which was previously allowed under Section 215 of the USA Patriot Act. The government must now identify with specificity the identity of a person, account, address, or personal device when requesting records. The law allows for the acquisition of data by two degrees of separation—or "hops"—from targeted individuals. If a centralized system in contact tracing is used, it is unclear whether the government may need to resort to this provision since it would likely have consent from individuals to collect and use the data.

The Privacy Act of 1974 also regulates the collection, use, and disclosure of personal data, but applies only to federal agencies (and their contractors), not to state or local agencies. 5 U.S.C. § 552a. The Act protects against disclosure of individually identifying "record[s]" that are kept within a "system of records." The Act limits disclosure of information "except pursuant to a written request by, or with prior written consent of, the individual to whom the record pertains." Certain disclosures are exempt from the Act's applicability. Pertinent disclosure exceptions are for records required to be disclosed under the. Freedom of Information Act (FOIA) or disclosures "to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual." A disclosure under FOIA, however, would not include information in "personnel and medical files and similar files" when disclosure "would constitute a clearly unwarranted invasion of personal privacy." FOIA Guide, 2004 Edition:

Exemption 6. If non-anonymized data are turned over to the federal or state governments, it is important to consider whether PII would be protected from disclosure under FOIA or state freedom of information laws.

Consent

User consent is a cross-cutting issue for evaluating many of the laws and regulations governing personal information privacy discussed in the prior sections. In general, privacy laws can be justified on the grounds that an individual should have the option to control, with various types and degrees of limitation, the collection, use, retention, and/or disclosure of information pertaining to that individual by others. As such, many privacy laws start from the premise that, absent an individual's consent, use or disclosure of that individual's PII is impermissible except for certain enumerated purposes deemed to outweigh the individual's privacy interests.

Consent, like agreements in general, can be manifest in different ways in specific circumstances. In some cases, an affirmative action—such as a signature—is needed to demonstrate consent. In other cases, inaction—such as declining to "unsubscribe" from receiving certain unsolicited emails—constitutes consent. Where a law requires a "written" signature, in all but a few contexts, the signature may be executed electronically. In the United States, that means the "signature" may consist of any of the following: "an electronic sound, symbol, or process," so long as it is "attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Electronic Signatures in Global and National Commerce Act (E-SIGN) (15 U.S.C. 7006).

The scope of a consent depends on what was deemed to be understood by the consenting party. That is least clear when the consent is inferred from inactivity, even if terms stating the consequences of inactivity have been provided. The scope of consent is most clear when the terms agreed to have been presented to or provided by the consenting party in a conspicuous, documented manner and a record exists of those terms. Courts uphold the validity of clickthrough agreements because users are deemed to review the terms to which they respond by clicking "I agree."

But where terms are ambiguous or confusing, buried in other text, or presented obscurely, the "I agree" action may not mean the user actually agreed to specific terms.

Terms of Use and Privacy Policies for apps are often written in complicated or nuanced language, with key points difficult to discern. Moreover, they are generally hard to read on a mobile device. Many users of mobile phone apps agree to such terms without even attempting to read or to understand them. As such, it is often questionable whether an app user has knowingly agreed to all the terms of those documents. Presentation of terms in large typeface, short sentences, simple language, and direct disclosures makes user consent more meaningful.

For contact tracing apps that collect PII and/or PHI, consent will overcome the restrictions of many if not most privacy laws, provided the consent is freely given, reflects a full understanding of the terms for use, collection, and disclosure of the information, and is confirmed by an affirmative act, such as a click that may be executed only upon a complete reading of Terms of Use and Privacy Policies. Whether consent may be deemed "freely given" in certain circumstances depends on contextual understandings of party relationships, including the employer-employee and government-citizen relationships.

Anti-discrimination and Individual Freedom Laws

Any measure taken to protect public health and safety must comply with the Constitution and civil rights laws, such as the ADA, that prohibit discrimination against persons in certain protected categories, such as race, gender, religion, or disability. In addition, certain implementations of DCTT could be challenged under a variety of individual freedom protections.

Anti-discrimination Laws

In general, it would be impermissible to use DCTT in a way that either targets or excludes people on the basis of their membership in one of these protected categories.

When motivated by animus against a protected class as defined by law and not narrowly tailored to advance a compelling government inter-

est, a discriminatory regulation would be considered unconstitutional under the Equal Protection Clause of the Fourteenth Amendment to the US Constitution. See *Jew Ho v. Williamson*, 103 F.10 C.C.N.D. Cal. (1900) (striking down a quarantine imposed by San Francisco in response to an outbreak of bubonic plague because it was racially motivated); see also *Church of Lukumi Babalu Aye v. Hialeah*, 508 U.S. 520 (1993) (supposed public health measure unconstitutional because it targeted the practices of one religion).

The risk of unintentional, yet illegal discrimination in using DCTT is a real possibility. Recent studies of infection rates among the population have revealed a larger-than-proportional infection rate among certain minority communities, such as Latinx, African American, and American Indian communities (NYC DOH 2020). Programs that target specific racial, ethnic, tribal, or religious groups may raise constitutional and other legal concerns.

Religious Freedom Laws

The use of DCTT may also raise concerns about religious freedom. For example, there may be religious objections to restrictions on gathering for worship, carrying a mobile phone, or the use of imaging technology. Under current Supreme Court precedent, generally applicable laws that do not discriminate against religion on their face do not violate the Free Exercise Clause of the First Amendment, even if those laws have an incidental effect on the exercise of religion. *Employment Div. Dept. of Human Resources of Oregon v. Smith*, 494 U.S. 872 (1990). These laws need not be justified by compelling government interest (the "strict scrutiny" standard of review); the government need only show that they are rationally related to a legitimate interest. On the other hand, laws that are not neutral and not of general applicability must be justified by compelling government interest and must be narrowly tailored to advance that interest if it burdens religious practices—a very tough hurdle to overcome. *Church of Lukumi Babalu Aye v. Hialeah*, 508 U.S. 520 (1993).

This general approach, however, is disrupted in some contexts by statutes adopted to provide greater protection to religious freedom. The federal Religious Freedom Restoration Act (RFRA) requires strict scrutiny for federal actions that burden religion, and many states have adopted "state RFRAs" that do the same for actions by state and local

governments. The Religious Land Use and Institutionalized Persons Act, which extends similar protections to persons confined to an institution such as a prison, jail, or mental health facility, may also be relevant. 42 U.S.C. § 2000cc.

Under either standard of review, courts will examine whether a government action imposes a substantial burden on religious exercise; if not, no religious freedom violation has occurred. Such a finding is unlikely for DCTT programs absent evidence that the government is using the digital information to take action against religious persons that is not necessary to avoid the spread of a serious disease. Nevertheless, legal challenges on religious freedom grounds cannot be ruled out.

Legislative Recommendations

- 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 uniformity of legal requirements.