FUTURE OF PRIVACY FORUM

JULY 2021

DIGITAL CONTACT TRACING TECHNOLOGY

Privacy and Equity Principles, Framework, and Stakeholder Proceedings

Dr. Rachele Hendricks-Sturrup
Research Director, Real World Evidence, Duke-Margolis Center for Health Policy, rachele.hendricks.sturrup@duke.edu

John Verdi
VP of Policy, Future of Privacy Forum, jverdi@fpf.org

ACKNOWLEDGMENTS

This paper benefitted from contributions and editing support from Katelyn Ringrose, former FPF Policy Fellow; Srivats Shankar, former FPF Intern; Kelsey Finch, FPF Senior Policy Counsel; Pollyanna Sanderson, FPF Policy Counsel; Juliana Cotto, FPF Policy Counsel; Christy Harris, FPF Director of Technology and Privacy Research; Jasmine Park, former FPF Policy Fellow; Dara Garcia, former FPF Intern, and Lauren Merck, FPF student contractor.

Support for this project was provided by the Robert Wood Johnson Foundation. The views expressed here do not necessarily reflect the views of the Foundation.

For questions about this project and FPF's Privacy and Pandemics Initiative, please contact info@fpf.org.

Table of Contents

Executive Summary

As part of its Privacy and Pandemics initiative, the Future of Privacy Forum (FPF), together with Dialogue on Diversity, the National Alliance Against Disparities in Patient Health (NADPH), BrightHive, and LGBT Tech, has developed a set of principles to support privacy and equity in the implementation of digital contact tracing technology (DCTT). The principles advise organizations implementing DCTT to commit to the following actions:

- Be Transparent About How Data Is Used and Shared
- Apply Strong De-Identification Techniques and Solutions
- Empower Users Through Tiered Opt-in/Opt-out Features and Data Minimization
- Acknowledge and Address Privacy, Security, and Nondiscrimination Protection Gaps
- Create Equitable Access to DCTT
- Acknowledge and Address Implicit Bias Within and Across Public and Private Settings
- Democratize Data for Public Good While Employing Appropriate Privacy Safeguards
- Adopt Privacy-By-Design Standards That Make DCTT Broadly Accessible

The principles build on FPF's previous work on our Privacy and Pandemics initiative. In response to the unresolved ethical, legal, social, and equity issues that may challenge the successful implementation and scaling of DCTT, we engaged leaders within the privacy and equity communities to develop actionable guidance for the successful implementation of privacy-preserving DCTT. We conducted multiple literature reviews, created a technical, foundational playbook, and compared existing frameworks.

Then, we engaged leading privacy, health, and human rights advocacy organizations in one-on-one, semi-structured interviews and two consensus workshops, using a modified Delphi method to explore, discuss, and answer key questions. We conducted a final two-hour workshop to present the preliminary framework of guiding principles to a larger group of experts.

This proceedings document describes the work of FPF and our invited experts. The group reached consensus views on many important issues, but specific views expressed in this proceedings document should not be attributed to a particular participant.

Background

COVID-19 has prompted government entities, regulators, industries, employers, and other public- and private-sector stakeholders to consider and support the development of DCTT as a tool to help contain the spread of the disease. Contact tracing is a disease surveillance process that is traditionally carried out by epidemiologists and public health practitioners, who conduct the tracing manually. DCTT was deployed globally and rapidly in 2020 when Google and Apple released their application programming interfaces (API) to several nations and their member states that wanted to implement DCTT via smartphone apps. In April 2020, FPF charted and compared DCTT apps and software development kits that were developed internationally. To date, several countries and nations, including the United States (US), have adopted the application programming interface (API) to enable exposure notification between Apple and Android users who may come in contact with one another, regardless of their location.

Accompanying DCTT was a promise to significantly improve the quality and speed of manual contact tracing and to privately notify individuals in real time of their COVID-19 exposure risk. The US Centers for Disease Control and Prevention noted, in 2020, that DCTT holds the potential to augment or improve manual contact tracing methods and procedures by:

- Decreasing the amount of time required for public health authorities to notify individuals of their potential exposure to a person(s) infected by a highly communicable disease such as SARS-CoV-2; and
- Improving case management and public health surveillance processes through improved exposure notification and integration of data captured electronically across multiple public health systems and personal mobile devices.

Although evidence has yet to confirm whether DCTT has fulfilled this promise, discussions in the public and private sectors continue to focus on creating and implementing digital solutions to address COVID-19. For example, as COVID-19 vaccine distributions began, more digital solutions emerged. This includes vaccine or health passport apps with digital exposure notification features, such as the V-Health Passport™, which uniquely links digital exposure notification with vaccination and other electronic health records. Examples of DCTTs in the US include COVIDWISE, developed by the Virginia Department of Health; CO Exposure Notifications, developed by the Colorado Department of Public Health & Environment and Colorado State Emergency Operations Center; and an Association of Public Health Laboratories platform, developed by epidemiologists in multiple states and the Metropolitan Washington Council of Governments, for exposure notification across neighboring state lines in the US (District of Columbia, Maryland, Virginia, and West Virginia). At the global level, there is Stopp Corona, developed by the Austrian Federal Ministry of Health, and Coronavirus-SUS, developed by the government of Brazil.

Below, we discuss the following:

1. Key privacy-related aspects of and considerations for DCTT;
2. Broad societal implications to DCTT implementation, including but not limited to the digital divide and/or digital exclusion; and
3. The process we used to develop our privacy and equity framework (see Appendices I and II) that can be used by DCTT developers and providers.

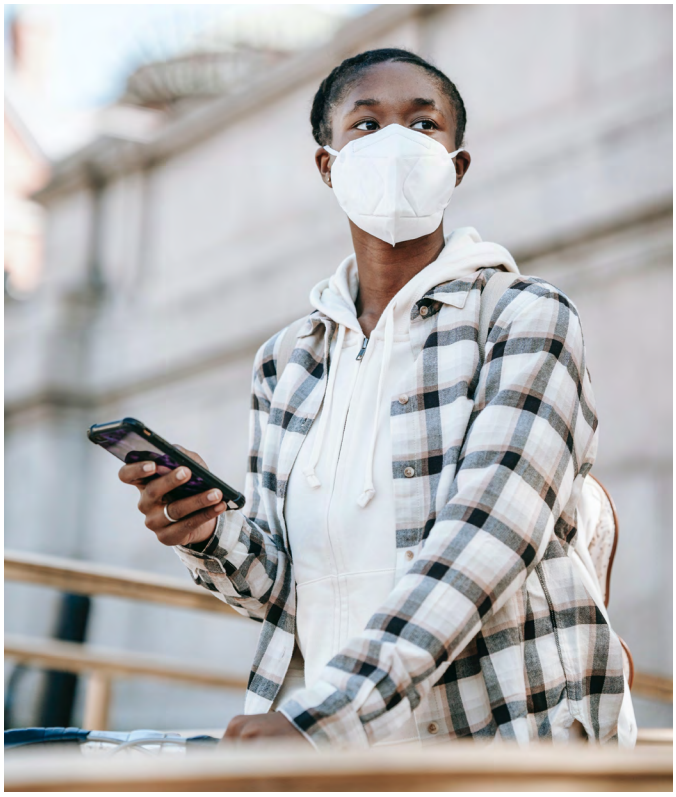
Privacy-Related Technical Aspects of DCTT

The Google/Apple API, adopted broadly in the US among DCTT developers, contains several privacy-by-design elements and privacy-preserving components. First, the API does not track users' locations. Instead, it relies on Bluetooth technology to detect whether two or more devices are near each other, but without disclosing the devices' actual map locations. Moreover, when the API is functioning, users' identities are unknown to Apple, Google, and other users. However, public health authorities may ask users for contact information through the API. Overall, the API promises to enable users who wish to privately send or receive automated exposure notifications for COVID-19.

An early, rapid Cochrane review of peer-reviewed studies, published in 2020, aimed to "assess the benefits, harms, and acceptability of personal digital contact tracing solutions" based on results from 12 studies published between January 1, 2000 and May 5, 2020 that met the reviewers' inclusion criteria. The review identified symptom tracking as an additional public health surveillance process that DCTT could improve. The authors sought to determine whether any of the studies identified privacy, ethical (e.g., equity), or safety issues or concerns for the different contact tracing approaches. Although none of the 12 studies contained qualitative evidence of ethical concerns, some of the studies identified privacy or safety concerns for different contact tracing approaches (see Table 1).

Table 1 presents several privacy considerations for DCTT from a technical standpoint, which includes protecting diagnosed users from contacts, snoopers, and authorities and sharing information with contact tracers working in public health agencies (contact tracing app used by contact tracers for data management). The table shows that DCTT contains foundational and technical limitations that are both expected and perhaps exclusive to the type of DCTT used. Several studies, such as the work of Stefano Tessaro at the University of Washington, examine the scientific validity and efficacy of digital exposure notification or DCTT. Other studies remain underway.

The National Institute for Standards and Technology (NIST) recently cited "privacy and cybersecurity concerns," "validation and verification," and "data and standards" as three of several challenges associated with implementation of proximity detection technologies such as DCTT. During NIST's January 2021 workshop, participants provided an overview of privacy considerations for DCTT, presented privacy-preserving protocols



for encounter metrics, and discussed privacy-by-design as infrastructural power for digital proximity detection during pandemics. For example, Dr. Naomi Lefkowitz, Senior Privacy Policy Advisor of the NIST Information Technology Lab, discussed how to apply the NIST Privacy Framework Core to exposure-notification technology. She focused on the framework core's governance, which includes organizational privacy values and policies as well as legal, regulatory, and contractual requirements, and recommendations for dissociated processing, which involves limited processing to prevent the identification of individuals. Key takeaways regarding privacy and equity were that developers of digital exposure notification/proximity detection solutions should adopt the following practices:

- Rely on operating environment, privacy/security properties, and stakeholder objectives as sources to inform the development of DCTT;
- Create DCTT solutions that cannot collect, process, or transmit any more data than what is necessary to achieve public health; and
- Leverage privacy-by-design to limit the accumulation of data and to reign in power asymmetries in situations in which privacy is power.

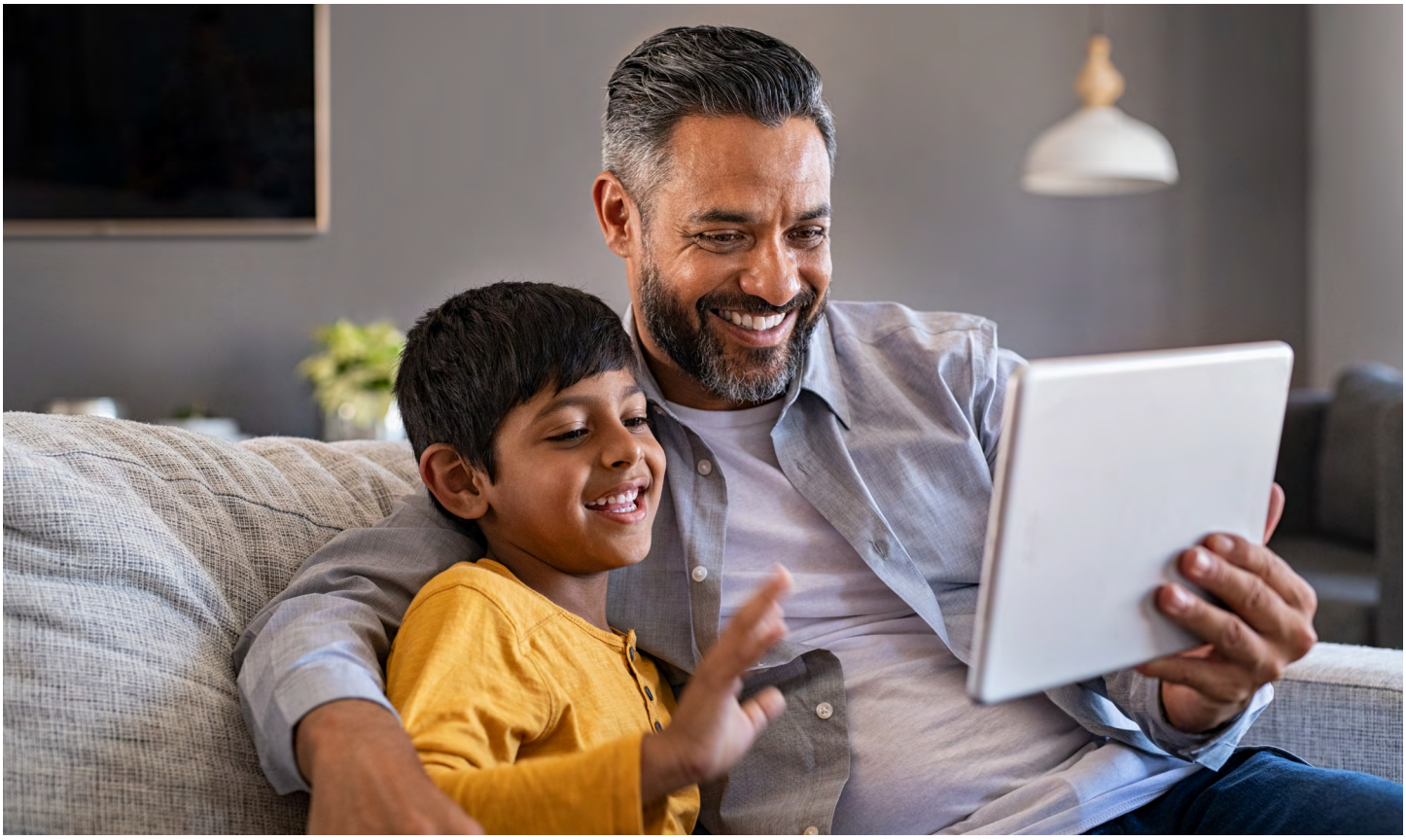
PRIVACY-RELATED TECHNICAL ASPECTS OF DCTT (continued)

Table 1. Privacy considerations for various digital contact tracing technologies (Anglemyer et al., 2020)

App/digital solution	Privacy from snoopers	Privacy from contacts		Privacy from authorities	
		Exposed user	Diagnosed user	Exposed user	Diagnosed user
Contact tracing app used by contact tracers for data management	Password protected only	Yes	Yes	No. Exposure status known to tracers	No. Diagnosis status known to tracers
Wearable RFID-enabled badge, wireless linkage to readers	Linkage attacks possible	Yes	Yes	Yes. Local affiliated researcher access only	Yes. Local affiliated researcher access only
Wireless ranging enabled node-device	Linkage attacks possible	Yes	Yes	Yes. Local affiliated researcher access only	Yes. Local affiliated researcher access only
RFID-enabled sensors	Linkage attacks possible	Yes	Yes	Yes. Local affiliated researcher access only	Yes. Local affiliated researcher access only

RFID: radio-frequency identification-enabled

Broad Societal Implications of DCTT



COVID-19 has exposed the pervasiveness of health disparities across the globe. In addition, stakeholders have had unequal experiences with data-driven technologies such as DCTT deployed as strategies to address the pandemic. Longstanding equity issues, such as the digital divide and/or digital exclusion, and the long-term consequences they engender, such as disenfranchisement, can hasten and exacerbate economic disparities and social exclusion for underserved, historically disenfranchised, and underprivileged populations. Therefore, when anticipating broad societal implications for DCTT, it is important to know what is needed to address obstacles to successful DCTT implementation and understand how privacy-by-design and privacy-preserving techniques can be leveraged to promote equity in DCTT implementation.

In early work on our Privacy and Pandemics initiative, FPF co-developed a DCTT privacy playbook, which contains a list of technical, foundational plays to support DCTT implementation. Yet, we at FPF and others have acknowledged that unresolved ethical, legal, social, and equity issues may challenge the successful implementation and scaling of DCTT. Therefore, we endeavored to engage leaders within the privacy and equity communities to develop actionable guiding principles and a framework to help guide the successful implementation of privacy-preserving DCTT.

Developing the Preliminary Privacy and Equity Framework

We began by conducting multiple literature reviews, in partnership with BrightHive, to create a technical, foundational playbook to help interested readers ensure responsible use of data collected from contact tracing apps. We compared frameworks addressing privacy considerations for DCTT implementation, focusing on relevant privacy principles, values, laws, and guidelines. The playbook was informed by insights and recommendations from FPF workshops, publications, and testimony; the Georgetown Beeck Center Data Governance Handbook; the Johns Hopkins Digital Contact Tracing book; law.MIT.edu privacy principles and related efforts; STAT news articles and commentary; and other COVID-19 data protection guidance and resources.

Later, also in partnership with BrightHive, we published a report in the *MIT Computational Law Report* to outline considerations on equity and fairness and encourage stakeholders to "to think about how DCTT can use in a trusted, service-integrated, and nondiscriminatory way and, subsequently, improve adoption." We offered initial recommendations on equity and fairness in DCTT implementation and highlighted legislative trends shaping DCTT initiatives across the US at the time of publication (August 2020).

Then, we engaged six privacy, health, and human rights advocacy organizations in one-on-one, semi-structured interviews and two consensus workshops, using a modified Delphi method to explore, discuss, and answer the following questions:

- How can contact tracing efforts, informed by digital exposure notifications, be designed and implemented to reflect equity, fairness, and privacy?
- How must DCTT be operationalized to minimize or eliminate individuals' or groups' fears of being tracked, deported, disenfranchised, displaced, or stigmatized?
- What have we missed? What are other important privacy and equity considerations to ensure the successful adoption and scaling of DCTT?

The semi-structured interviews involved FPF staff with subject matter expertise and leaders of each privacy, health, and human rights advocacy organization. As FPF staff and the leaders discussed these questions, two FPF staff members took notes in order to identify and compare shared and potentially unshared themes regarding values. During each two-hour workshop, five of the six organizations interviewed discussed these themes (one organization withdrew from the initiative due to time constraints) to reconcile terminology across interests, create or endorse definitions, curate related resources, and draft the preliminary framework of guiding principles that prioritize privacy and equity.

Final Workshop

We conducted a final two-hour workshop to present the preliminary framework of guiding principles to a larger group of individuals within and outside of FPF (total of 17 attendees; see roster in Appendix I). During the first hour of the workshop, we presented the preliminary privacy and equity guiding principles and framework. During the second hour, FPF staff engaged workshop attendees in three breakout sessions, focused on considerations for academia, government/civil society, and industry. Staff and participants explored the following questions:

- Are these principles enough, or do we need more?
- How might inequitable DCTT implementation disadvantage or benefit certain groups?
- How might underrepresented groups engage in the development and implementation of DCTT?
- Is auditing of DCTT necessary, and if so, should it be mandatory?
- How might these principles backfire against or further inspire DCTT implementation?
- How might individuals and entities monitor and track the release of various DCTTs domestically and internationally and understand their value through a human and civil rights lens?

Appendix II shows the final version of the guiding privacy and equity principles and framework to support DCTT implementation. We summarize the feedback and perspectives of attendees from each breakout session (academia, government/civil society, and industry) below, to inspire future cross-sectoral and multi-stakeholder engagement on the topic of privacy-protective, equitable DCTT implementation.

Summary of Final Workshop Proceedings

We identified three cross-cutting themes regarding actionable next steps from the academia, government/civil society, and industry breakout sessions:

1. Involve local community stakeholders in the development and execution of DCTT data collection, use, retention, and auditing policies to ensure thoughtful, responsible DCTT implementation among socially and economically vulnerable communities or populations.
2. Apply the privacy and equity principles as a lens through which stakeholders can further develop current DCTT implementation practices and policies, to foster trust and engagement among socially and economically vulnerable communities or populations during DCTT implementation.
3. Engage in and support research and other initiatives that address or fill gaps in scientific evidence, policy, and practical knowledge regarding privacy and equity in DCTT implementation.

Workshop participants discussed issues related to equitable implementation of DCTT in the context of academia, civil society/government, and in industry. As described below, participants highlighted risks, opportunities, uncertainty, and opportunities for future work that can support the public health and clinical benefits of DCTT while promoting equity and meaningful privacy safeguards.

Academia

Conversations about use of DCTT in academic settings are often grounded in the assumption that every individual has, wants, or can gain access to DCTT. But that assumption is incorrect.

For instance, individuals of low socioeconomic status often face financial hardships, yet it would be erroneous to assume that financial hardship is the only reason that individuals might not own or use smartphone technology. Low technology readiness or lack of experience, familiarity, and comfort with using a smartphone may be additional reasons that individuals might choose to not use a smartphone or smartphone-based technology such as DCTT. Therefore, academic stakeholders should not assume that every individual has or even wants access to a smartphone, let alone DCTT. Many individuals and communities may have reservations about the implementation of institutional data-collecting initiatives. The novelty of DCTT does not change individual and generational trauma from past events, and DCTT initiatives may still encounter mistrust in places where a technology resembles systems that have been previously abused to the detriment of community stakeholders.

Diverse representation in feedback regarding DCTT implementation in the academic sector is necessary to capture strategies that ensure equitable, effective implementation. This representation should exist

both at a high level (e.g., among policymakers, elected officials, and DCTT developers) and on a smaller scale in local governments, community leadership, and local schools. One way to get multiple perspectives and enhance inclusion and representation may be through the creation of local, multi-stakeholder committees tasked with overseeing and disseminating technical, foundational recommendations for local DCTT implementation.

Conversations about DCTT data privacy currently derive heavily from Europe, with less consideration of Asia-Pacific Economic Cooperation nations or local communities in the US. Therefore, DCTT developers and local adopters of the technology need to explain the technology in ways that people can understand. Taking the time to educate users on how DCTT products work and which personal information an initiative will and will not collect and analyze demonstrates respect. Simply instructing people to use a certain technology or offering impersonal disclaimers about the use of contact tracing may not be as effective as taking the time to explain why certain data is useful and exactly how it will be used. Holding local focus groups may help to build trust. The education sector can be a bridge to build trust and bolster inclusion among community stakeholders.

Thoughtful, responsible implementation efforts are also key. Stakeholders should not make decisions about DCTT development and implementation lightly. To effectively and responsibly use DCTT, developers and implementers must be mindful of and acknowledge people's potential reservations and fears regarding the technology. For instance, potential law enforcement access to DCTT data generated in academic settings could create new challenges in building and sustaining trust, especially in communities with complex histories and interactions with law enforcement. Thus, questions such as who has access to DCTT data require thoughtful consideration, as such questions, protection gaps, and risks likely remain unaddressed among certain vulnerable populations that engage with law enforcement in academic settings.

The generation, collection, processing, and use of end-user data from devices is not comprehensively regulated in countries such as the US. In addition, widespread auditing on a global (or even national) scale will likely be more difficult to manage than smaller-scale efforts on a local or school-district level. Therefore, stakeholders should conduct local exploration and development activities to identify best practices for thoughtful, responsible DCTT implementation, data collection and use, and auditing and monitoring in academic settings. Local exploration and development activities could involve, for example, identifying uniform privacy and equity standards and best practices for the following issues:

1. Who should monitor and audit DCTT efforts locally to ensure privacy and equity standards and to prevent the misuse of DCTT data;
2. Ensuring that DCTT does not exacerbate but, rather, addresses inequities in local communities;
3. Determining the scale at which auditing and monitoring processes and procedures should occur; and
4. Delegating auditing and monitoring tasks to internal andt/or independent and neutral third parties.

Local exploration and development activities should also identify potential disparities in location and/or inconsistencies in internet availability or access to resources needed to comply with technology standards for local DCTT implementation and use. Prior to implementing a DCTT policy, K-12 school administrators should also consider whether children or students would have reasonable access to DCTT-enabling technology and the age at which DCTT is appropriate for use among children.

Finally, support for innovation is an important consideration. Whether the DCTT privacy and equity principles will ultimately create more regulations that stifle DCTT development and implementation is unclear. The following questions remain:

1. Could the privacy and equity principles lead to the development of regulations that hinder DCTT innovation?
2. Might DCTT creators and developers become less motivated to develop novel DCTTs if more privacy rules or regulations exist?
3. If the privacy and equity principles are or could be implemented successfully, would concerns about stifling innovation matter?

These questions offer another yet unique angle for exploring how stakeholders can thoughtfully implement DCTT.

Government/Civil Society

The privacy and equity principles create an important path toward establishing trust in government and civil society sectors that implement DCTT. For this reason, stakeholders may find that the principles offer initial confidence to users with regard to protection. Perhaps through the endorsement and implementation of the privacy and equity principles, trust in DCTT could grow, which might increase the likelihood that governments and individuals will adopt DCTT during and after COVID-19.

However, high-level discretion and granular guidance are needed to prevent unauthorized uses of DCTTs and associated data and to ensure DCTT data-purpose limitation in government and civil society. For example, although opt-in and opt-out choices regarding minimum necessary DCTT data collection and use are important, these choices could inspire the consideration and development of additional DCTT data-collection and data- or device-use protections. Yet, although perfection in this regard is aspirational, it should not become the enemy of good DCTT development and implementation. Each step toward establishing privacy and equity in DCTT is important, and enforceable privacy laws in the US, such as the California Consumer Privacy Act, are good, reasonable first steps that stakeholders can improve over time.

Auditing procedures and standards for DCTT development and implementation could be necessary today and, in the future, to advance a DCTT agenda with proper technical and procedural oversight. If done correctly, audits could determine the level and extent to which stakeholders have adhered to the privacy and equity principles. A legislatively mandated, independent third-party auditing process could both ensure oversight and improve trust in the system.

It is equally important to effectively communicate with diverse communities, to uphold notions of transparency, safety, empowerment, and confidence. Tiered privacy choices and solutions are important so that users may opt in or out of specific DCTT features. For example, users should be able to opt in to exposure notification without feeling coerced or compelled to opt in to new vaccine passport features when they become available on the same DCTT tool or device. Not only does this promote user choice and empowerment; it promotes accountability for DCTT oversight entities and regulators to scrutinize and enforce protections. Such choices also provide opportunities to educate DCTT developers on privacy-by-design standards and features.

When stakeholders consider how access to and use of DCTT could benefit or disadvantage certain groups in civil society, it is critically important to engage people with lived experience and their community leaders in anchor institutions. Such institutions might include local churches and libraries. By engaging these communities and learning about their struggles, stakeholders can explore ways to address past transgressions against the community and remove structural barriers in order to bolster the community's confidence in using and relying on DCTT during and after the pandemic.

The privacy and equity principles are a reasonable first step toward achieving transparency, use specification, and good practices in DCTT, if stakeholders in government and civil society apply the principles. Nonetheless, there is a need for open dialogue with local communities to identify possible implementation challenges. With regard to equity and fairness, discussions with local communities should center on issues related to access to smartphones or other preferred technology that would house DCTT. Discussions should also address how policymakers and governments could overcome local barriers in internet access and other key infrastructure needed to support trusted DCTT engagement.

Industry

The privacy and equity principles are a wise starting point to create and inform ethical industry practices regarding DCTT. However, further exploration is warranted to identify barriers to and potential impacts of industry-led DCTT among vulnerable populations. One example of such exploration is to determine how the privacy and equity principles can apply to COVID-19 patient- or user-centered research, again focusing on outcomes among members of socially vulnerable populations or communities. Stakeholders can also apply the privacy and equity principles to industry policies to understand the policies' effects in general user settings.

Additional research questions for exploration among or with DCTT industry stakeholders include the following:

- Does existing DCTT data describe or suggest potential risks to vulnerable communities that could result from DCTT implementation practices?

- Whose perspectives are missing among vulnerable populations (e.g., senior or elderly adults, citizens, prisoners, etc.) in terms of how DCTT practices can benefit or harm them?
- Do we currently have data to demonstrate or describe outcomes for individuals who have been tracked through means other than DCTT?
- Do DCTT industry best practices exist that the privacy and equity principles can further refine?
- Which industry-led multi-stakeholder engagement initiatives have already begun to address privacy and equity concerns and issues in DCTT implementation?

Evidence generated in attempts to answer these research questions might inform the creation and development of DCTT implementation policies, guidelines, procedures, and practices tailored to diverse communities or specific societal contexts. Operationalizing the privacy and equity principles amid stark cultural differences and issues of discrimination in society is a major challenge to consider. Further research in this regard could create learning opportunities to help DCTT industries and developers understand, through a human and civil rights lens, the consequences of their DCTT implementation efforts and practices.

Another important consideration for DCTT industry stakeholders is whether and how DCTT data-collection policies, processes, and procedures should be audited, and if so, who should conduct the audit, either publicly or privately. Currently, there is no well-established or widely disseminated or accepted protocol for this. Stakeholders could develop or tailor auditing processes in terms of new or existing 1) DCTT data-reporting systems that might have established policies, processes, and procedures regarding data collection, processing, analysis, sharing, and use; and 2) technical and foundational best practices regarding data retention, purpose limitation, and data minimization. The privacy and equity principles could provide an added human and civil rights lens to both of those DCTT developments that can be subject to auditing.

DCTT data-retention policies and practices should include a data-retention schedule, especially if DCTT users' minimum necessary personal information is tracked or traced. When the personal data is no longer beneficial for public health purposes, then the data should be disposed of or deleted. Data-retention schedules for personal data privacy management are important for several reasons. First, retention schedules can help build trust with vulnerable populations who wish or are compelled to use DCTT for various daily purposes. Second, retention schedules can provide assurance that their personal data will not be kept indefinitely or used for secondary purposes beyond users' consent or the scope of public health. Third, retention schedules can help prevent excessive data accumulation that results in data graveyards; these graveyards can lead individuals or parties unaware of the original or intended purpose of the data to misuse the data in the future.

Although assuring DCTT users of how the process will use, process, or share their data could motivate underrepresented and socially vulnerable groups to engage in the development and implementation of DCTT, it is important to acknowledge that data on the effectiveness of DCTT is still emerging. As this evidence continues to emerge, the privacy and equity principles can help guide future studies, analysis, and implementation testing.

Another challenge in the DCTT implementation process involves understanding the role of some DCTT developers as nonclinical or nonpublic health intermediaries. Given that many DCTT developers are independent tech companies, current and potential users of DCTT may not fully trust that the data they provide or exchange via the DCTT platform will remain confidential. Moreover, the lack of a comprehensive federal privacy law in the US might preclude individuals from feeling confident in the privacy of their personal information shared or exchanged via a DCTT platform. Therefore, DCTT privacy laws are a necessary step toward ensuring the successful implementation of DCTT activities today and in the future.

Some industries profit on the resale or licensing of previously collected data from their technology users. DCTT users may suspect that the DCTT industry is no exception to these data monetization practices. Therefore, to establish trust and confidence among users, DCTT industry players could help develop and publicly adopt or endorse best practices that align with the privacy and equity principles and make clear whether DCTT data will be subject to pre-existing DCTT industry revenue models.

Appendix I: Roster of Final Workshop Attendees

Claire Bowen *Lead Data Scientist, Privacy & Data Security* Urban Institute	**Andrew Crawford** *Policy Counsel, Privacy and Data Project* Center for Democracy & Technology	**Joanne Charles** *Principal Corporate Counsel* Microsoft
Dr. Cheryl Brown *Associate Professor & Department Chair* University of North Carolina at Charlotte	**Jessica Kallin** *Student Data Privacy Trainer* Utah State Board of Education	**Maithri Vangala** *Former Director of Community Engagement* BrightHive
Kim Crouch *Counsel* General Motors	**Whitney Phillips** *Chief Privacy Officer* Utah State Board of Education	**Dr. Natalie Ortiz** *Former Director of Data Collaboration Services* Brighthive
Erica Finkle *Director, Privacy & Data Policy* Facebook	**Lindsay Palmer** *Privacy Research Specialist* TrustArc	**Sumeera Arshad** *Program Manager* Santa Clara County
Carlos Gutierrez *General Counsel* LGBT Technology Partnership & Institute	**Nia Peters** PwC	**Allen Miedema** *Executive Director for Technology* Northshore School District
Ellie Bessette *Director of Programs* LGBT Technology Partnership & Institute	**Karen Vinelola** *Director, Privacy & Ethics, Products & Technology* PwC	**Mark Szpak** *Retired Partner and Of Counsel* Ropes & Gray LLP
Noe Leiva *Program Manager for AI Ethics Projects* IBM	**Dr. Alex Carlisle** *Founder, Chair, & CEO* National Alliance Against Disparities in Patient Health	**Cristina Caballero** CEO *Dialogue on Diversity*

Appendix II: Privacy and Equity Actionable Guiding Principles and Framework for Digital Contact Tracing Technology Implementation

PRINCIPLE 1

Be Transparent About How Data Is Collected, Used, and Shared

DCTT providers may use and share contact tracing data for public health or related purposes. Historical and present-day evidence indicates that sensitive data can be used by powerful entities, like law enforcement, in discriminatory ways, subjecting certain groups of individuals to oppression, violence, and other extreme social circumstances. Moreover, if the technical precision or accuracy of DCTT is unclear or not well evidenced, it is possible that DCTT could prompt actions based on false positives or inaccurate contact tracing, like law enforcement actions against socially vulnerable populations.

DCTT users should be made aware of how their data is being collected, used, and shared through prominent, understandable, and accessible statements. For example, data collection, use, and sharing transparency notices can be provided prior to DCTT installation through app store notices, upon downloading or installation through in-app terms of service disclosures, or upon first-time usage of the DCTT via "just-in-time" mobile app notifications. Notices and/or privacy settings should also explicit state when and the duration of time for which sensitive data is collected.

PRINCIPLE 2

Apply Strong De-Identification Techniques and Solutions

DCTT providers should apply strong privacy protection techniques and solutions to prevent malicious and/or unauthorized parties from leveraging sensitive data collected via DCTTs in ways that are misaligned or conflict with the spirit of public health, or that introduce risk of harm. Organizations can implement technical, policy, contractual, or legal controls over data to help accomplish this. Controls can include strong de-identification techniques, data security safeguards, data decentralization, and privacy firewalls for exposure notification data. For example, strong de-identification techniques can involve the removal of direct and known indirect identifiers to obscure or mask real world identities. Data security safeguards and privacy firewalls include technical permissions that limit access to authorized individuals, as well as organizational and legal controls that prohibit third parties from identifying or re-identifying DCTT users. Lastly, data decentralization means that exposure notification data remains on the device and, therefore, the identities of the device owners remain undisclosed upon exposure notification.

Interoperable data architectures and data types that contain individual user-level information, such as age and gender data paired with geolocation data, should be safeguarded through the use of appropriate and robust security protections that operate effectively across multiple data architectures. Without such protection measures, there is a risk of, or potential for, data misuse or abuse, lack of data minimization, and thus limited user adoption and/or infectious disease testing compliance.

PRINCIPLE 3

Empower Users Through Tiered Opt-in/Opt-out Features and Data Minimization

DCTT participation should be voluntary (versus mandatory or compulsory) and DCTT users should typically be given the choice to opt into specific DCTT features (i.e., enabling "active" [opt-in] versus "passive" [nested or foundational; opt-out by default] participation modes).

By default, DCTT should collect only the minimum necessary data to provide users with the service. Additional features that collect more user data should prompt DCTT users to opt in or opt out of further data collection and sharing. Meaningful and impactful opt-in/opt-out options should be offered and DCTT users should be able to easily access these options.

PRINCIPLE 4

Acknowledge and Address Privacy, Security, and Nondiscrimination Protection Gaps

There may be limited enforceable administrative protections in place to monitor and regulate organizations' or service providers' privacy, nondiscrimination, and surveillance practices. Therefore, DCTT developers and institutional adopters of DCTT should publicly endorse an ethical code, standard, playbook, and/or framework that champions diversity and equity in DCTT and be held accountable to such standards. This might include, for example, FPF and BrightHive's

"Responsible Data Use Playbook for Digital Contact Tracing," Lo and Sim's "Ethical Framework for Assessing Manual and Digital Contact Tracing for COVID-19," or the National Association of County and City Health Officials' "Guide to Community-Based Workforce Principles for Contact Tracing." DCTT users are or should be encouraged and empowered to actively participate in both the development and implementation of such ethical codes, standards, and/or frameworks.

PRINCIPLE 5

Create Equitable Access to DCTT

Taking into account that some devices might be more compatible with certain DCTTs than others, it is important for developers to avoid tying a particular type of device to the most beneficial DCTT features. When creating equitable (versus equal) access to DCTT, it is important to account for and address the unique structural and procedural barriers individuals or groups might experience when seeking access to the benefits of using DCTT. Playing a part in facilitating equitable access to personal devices and infrastructures that are necessary for DCTT adoption and use is essential. For example, creating DCTTs that function without the need for wireless internet service or that are compatible with both older and newer mobile device versions can ensure that DCTT broadly reaches individuals, regardless of their economic status.

PRINCIPLE 6

Acknowledge and Address Implicit Bias Within and Across Public and Private Settings

It is important to acknowledge the current reality and impact of bias that exist across a multitude of important settings, like healthcare or public health settings, and address scenarios in which DCTT might expose, perpetuate, or even exacerbate social bias within those settings. As individuals or groups subject to implicit bias in those settings may encounter case mismanagement and/or discrimination, they are more likely to avoid such settings as a result, despite their importance and the importance of DCTT for managing public health during pandemics. For example, if a socially marginalized individual or group routinely encounter(s) embarrassment, fear, or shame when seeking healthcare services within a biased public health system, then that individual or group may likely feel compelled to not trust or engage in a DCTT program that is implemented by or within that system. Therefore, acknowledging and addressing implicit bias within and across settings in which DCTT is implemented could increase the likelihood that individuals feel safe to engage in DCTT.

PRINCIPLE 7

Democratize Data for Public Good While Employing Appropriate Privacy SafeGuards

To the extent possible, data should be democratized to offer benefits to public health programs and infrastructures. DCTT data can often be shared in a limited, de-identified way to promote these goals. Data can be shared with trusted research partners, managed as part of Community Health Information Network, or, in rare cases, made publicly available. Government and other relevant entities should implement strong measures to ensure privacy, particularly if DCTT data is made publicly available or broadly accessible.

Public policies should support and protect use of DCTT data for public health research by incorporating or endorsing strong data governance processes, practices, and procedures. For example, such processes, practices, or procedures could include identifying the minimum necessary categories of data that should be made available; applying technical, contractual, and/or procedural safeguards to prevent unreasonable disclosures of personal information; and ensuring DCTT user data is safeguarded through the use of strong encryption or other data security standards.

PRINCIPLE 8

Adopt Privacy-By-Design Standards That Make DCTT Broadly Accessible

Developers should adopt privacy-by-design design standards that can also ensure broad user access to DCTT. Such standards should ensure that the benefits of DCTT can be maximized to serve the public, but without compromising, by design, the privacy of and equity among DCTT users in the process.

Definitions

1. **DCTT:** Technology used for the purpose of detecting potential exposure to disease or infection. This includes applications tracing user movement and health status, and correlating data across multiple users to identify potential exposure.
2. **DCTT User:** An individual using DCTT on or through a personal device for public or private purposes.
3. **Data Minimization:** Data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. (GDPR Chapter 2, Article 5)
4. **De-Identification:** The process of removing personally identifiable information from data collected, stored, and used by organizations. (Future of Privacy Forum, A Visual Guide to Practical Data De-Identification [April 2016])
5. **Pseudonymization:** The process through which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact. (Future of Privacy Forum, A Visual Guide to Practical Data De-Identification [April 2016])
6. **Sensitive Data:** Data that is subject to specific processing conditions that render the data identifiable in the following contexts: 1) data revealing racial or ethnic origin, political opinions, religious, or philosophical beliefs; 2) genetic data, biometric data processed solely to identify an individual; 3) health-related data; 4) data concerning a person's sex life and sexual orientation; and 5) precise geolocation. (adapted from Article 4(13), (14) and (15) and Article 9 and Recitals (51) to (56) of the GDPR; also adapted from Section 14 of the California Privacy Rights and Enforcement Act)
7. **Decentralization:** The process in which available information is split into pieces and stored in various parts (mobile agents, edge computing centers, etc.) of a network instead of storing everything on a central server; in addition, no single entity has full control or the complete information. (Shubina et al. 2020)

CASE SCENARIO 1

An LGBT Community in Seoul, South Korea

During the early months of the COVID-19 pandemic, lesbian, gay, bisexual, and transgender (LGBT) persons in South Korea were accused of spreading COVID-19 after the government began to relax restrictions in early May of 2020, permitting bars and other social venues to reopen. Several new COVID-19 cases appeared thereafter and were traced to nightclubs in Itaewon, a Seoul city area known for its cosmopolitan dining and nightlife and that has been described by the media as a social center or safe space for "gay clubs." The mayor of Seoul stated that those "exposed who do not come forward for testing will be visited at home accompanied by police," which some fear puts LGBT populations at risk of discrimination and speculation about individuals' sexuality as a result of such tracing efforts. Thoreson, 2020, Human Rights Watch

CASE SCENARIO 2

Unresolved Tensions from the AIDS Era in the USA

Stories of unresolved tensions between contact tracers and the gay community in San Francisco, California persist today after nearly 40 years. Since the 1980's, contact tracers and gay rights lawyers have expressed that the effects of widespread, public health agency-enforced contact tracing efforts for the HIV/AIDS virus have caused the gay community to oppose contact tracing. Identifying individuals with exposure to HIV/AIDS can and has led to job loss, housing loss, and loss of other essential needs and services among the gay community.

Drawing on several stories and lessons learned regarding unresolved issues of mistrust among the gay community in public health agencies, a KQED reporter concluded that, today, local, state, and county public health departments are "building bridges with the affected populations by partnering with community groups" that have trusted relationships with the gay community. Dembosky, 2020, KQED

CASE SCENARIOS 1 & 2: *LESSONS LEARNED*

Case Scenarios 1 & 2 highlight why it is important to apply the following principles:

- **Principle 4: Acknowledge and Address Privacy, Security, and Nondiscrimination Protection Gaps**

  DCTT developers and institutional adopters of DCTT can foster trust by publicly endorsing and holding themselves accountable to an ethical code, standard, playbook, and/or framework developed with direct input from communities with a history of abuse or mistrust in certain institutions.

- **Principle 6: Acknowledge and Address Implicit Bias Within and Across Public and Private Settings**

  DCTT developers and institutional adopters of DCTT must anticipate and address current or possible scenarios in which DCTT might expose, perpetuate, or exacerbate harmful biases in a range or multitude of private and public settings to help ensure that individuals feel safe and protected from downstream harm or misfortune that might ensue due to implicit bias within a system or setting.

- **Principle 8: Adopt Privacy-By-Design Standards That Make DCTT Broadly Accessible**

  Privacy-by-design features or standards, like anonymous exposure notification, prompts individuals to make choices privately about monitoring and controlling their personal behaviors, circumstances, communication with others, and whereabouts following exposure to a communicable disease.

KEY TAKEAWAY

Contact tracing efforts to monitor the spread of communicable diseases in socially vulnerable groups can place those groups at risk of discrimination or ostracism at home or within their communities. Those populations may suffer the greatest, from a social and economic standpoint, and may be less likely to engage in any technology, including DCTT, that might disclose their private social affiliations and whereabouts.

CASE SCENARIO 3

An African community in Guangzhou, a southern city in China

Members of an African community in Guangzhou experienced discrimination after the government of China provided facially neutral warnings on social media against imported coronavirus. Guangzhou authorities stated that five Nigerians had tested positive for COVID-19, tracing coronavirus risk to Guangzhou's Yuexiu and Baiyun areas that are known to be home to predominantly African communities. A CNN news article stated that members of this African community were evicted from their rental homes and refused hotel service, despite the community members' claims of having no recent travel history or known contact with COVID-19 positive individuals. Many members of this African community rely on short-term business visas and travel between Africa and China several times a year.

Hostility against the African residents predated the emergence of COVID-19 in the city, but worsened during the pandemic. Individuals with "African contacts" were mandated to self-quarantine. The US Consulate in Guangzhou warned African-Americans to avoid traveling to Guangzhou amid the growing hostility. The US Consulate warned, "... police ordered bars and restaurants not to serve clients who appear to be of African origin." Marsh, Deng, and Gan, 2020, CNN; *U.S. Consulate General Guangzhou, People's Republic of China [2020, April 13]:* Discrimination against African-Americans in Guangzhou

CASE SCENARIO 4

A Muslim Community in Cambodia

The Cambodian Health Ministry named, on its official social media webpage, specific groups of individuals who were reported to have contracted COVID-19 after contact tracing revealed "no signs of transmission between people in their [local] communities. One of the specified groups was named as "Khmer Islam." It was reported that the social media post led to an "outburst" of discriminatory and hateful comments and gestures against Cambodia's minority Muslim communities both online and daily at markets, shops, and other public areas. Following these events, a Cambodian government spokesperson requested that the media refrain from providing identifying information about persons infected with COVID-19. Chhin, 2020, Human Rights Watch; Penh, 2020, VOA

CASE SCENARIOS 3 & 4: *LESSONS LEARNED*

Case Scenarios 3 & 4 highlight why it is important to apply the following principles:

- **Principle 4: Acknowledge and Address Privacy, Security, and Nondiscrimination Protection Gaps**

  DCTT developers and institutional adopters of DCTT can foster trust by publicly endorsing and holding themselves accountable to an ethical code, standard, playbook, and/or framework developed with direct input from communities with a history of abuse or mistrust in certain institutions.

- **Principle 6: Acknowledge and Address Implicit Bias Within and Across Public and Private Settings**

  When powerful entities like health or governmental authorities publicly attribute a communicable disease to a hyper-segregated area or group of persons that frequently travel to an area, it can appeal to or exacerbate individuals' harmful biases against those hyper-segregated or traveling groups. DCTT developers and users should develop and implement DCTT and data reporting strategies that safeguard against downstream effects of implicit and harmful biases, like disenfranchisement and hateful remarks, and protect the well-being and reputation of hyper-segregated communities or groups that are known to travel to certain areas of a community.

- **Principle 7: Democratize Data for Public Good While Employing Appropriate Privacy Safeguards**

  When minimum necessary data is collected and shared publicly, it can help prevent individuals from becoming socially targeted or mistargeted in harmful ways based on their personal affiliations, biological attributes, or other individuals' inherent biases and assumptions.

KEY TAKEAWAY

DCTT should not render groups that share certain characteristics or social affiliations, as targets for law enforcement, media defamation, or public shame. DCTT developers, policymakers, and other powerful stakeholders, including the media and social media companies and users, should anticipate potential misuses of contact tracing data. This should be done with the intent to safeguard vulnerable populations or individuals from social ostracism or discrimination based on religious affiliation, immutable characteristics, or other personal attributes.

CASE SCENARIO 5

A COVID-19 Contact Tracing App in North Dakota, USA

The Care19 app, a voluntary app developed by ProudCrowd, a company in North Dakota, was one of the first contact tracing apps to be implemented in response to the COVID-19 pandemic. The app was officially endorsed by North Dakota and South Dakota state government officials. Later, Jumbo Privacy, a tech privacy company, discovered that the Care19app contained code that sends app users' location and identification data to local and international third-party companies, including companies involved in commercial advertising. While the app contained this code, the app's privacy statement told users that their location data would "not be shared with anyone, including government entities or third parties, unless you consent or ProudCrowd is compelled under federal regulations." Groves, 2020, USA Today

CASE SCENARIO 5: *LESSONS LEARNED*

Case Scenario 5 highlights why it is important to apply the following principles:

- **Principle 1: Be Transparent About How Data Is Collected, Used, and Shared**

  If DCTT users are fully aware about if and how personal data is collected, used, and shared with third parties, then they are able to make informed choices regarding with whom they wish to share personal data. This protects the interests of not just DCTT users, but also DCTT developers that aim to deliver high standards of user/customer service.

- **Principle 3: Empower Users Through Tiered Opt-in/Opt-out Features and Data Minimization**

  Tiered opt-in/opt-out features and data minimization give DCTT users the power of choice to engage in ways that are best suited to their privacy preferences, personal well-being, and interests. DCTT companies or developers should carefully audit code they intend to adopt or use to ensure that they are not misleading themselves, their users/adopters, and regulatory authorities in their privacy statements and policies.

KEY TAKEAWAY

Privacy policies, terms of use agreements, and similar notices should be transparent, accurately reflect DCTT developer's privacy practices, and be written at broadly accessible reading levels. Privacy policies should not contain intimidating jargon, provisions, or terms that are difficult for most users to comprehend or interpret regarding an app's privacy practices. Such notices should not contain coercive terms that pressure users to opt in to less private features, especially if users need, heavily rely on, or are required to use the app for personal, legal, or other essential purposes. App developers, including DCTT developers, should carefully audit code they adopt or procure to ensure that the code adheres to their internal privacy standards, policies, and terms as well as app store rules and the privacy expectations of their users/adopters.

Key US Legislative Proposals Regarding Digital Contact Tracing Technology

State Bills

- **New York:** An act to amend the public health law, in relation to the confidentiality of contact tracing information (A10500C/S8450C)
- **New York:** Relates to requirements for the collection and use of emergency health data and personal information and the use of technology to aid during COVID-19 (A10583/S8448)
- **California:** Personal information: contact tracing (AB660; AB814)

Federal Bills

- COVID–19 Consumer Data Protection Act of 2020
- Public Health Emergency Privacy Act
- Exposure Notification Privacy Act
- Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act)
- Public Health Emergency Privacy Act
- Secure Data and Privacy for Contact Tracing Act

Summary of DCTT Legislative Efforts

- FPF's Summary of Additional US Legislative Trends as of August 2020

Key Resources Regarding Privacy and Equity in DCTT Implementation

- Digital Contact Tracing: A Playbook for Responsible Data Use
- Digital Contact Tracing and Data Protection Law
- Private Lives and Public Policies, Confidentiality and Accessibility of Government Statistics
- A Taxonomy of Definitions for the Health Data Ecosystem
- Rights in the time of COVID-19, Lessons from HIV for an effective, community-led response
- Technology in Conflict: How COVID-19 contact tracing apps can exacerbate violent conflicts
- Contact Tracing Apps: Extra Risks for Women and Marginalized Groups
- Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic
- A Virtual Roundtable on COVID-19 and Human Rights with Human Rights Watch Researchers
- Are Contact-Tracing Apps the Answer? Lessons the US Can Learn From Other Countries
- Context before code: Protecting human rights in a state of emergency
- Responsible Data Use Playbook for Digital Contact Tracing
- Ethical Framework for Assessing Manual and Digital Contact Tracing for COVID-19
- A Visual Guide to Practical De-Identification
- Best Practices for Consumer Wearables & Wellness Apps & Devices
- Norton Rose Fulbright live and comprehensive survey or summary of principal regulatory and policy issues across key international jurisdictions

The Future of Privacy Forum (FPF) is a catalyst for privacy leadership and scholarship, advancing responsible data practices in support of emerging technologies. FPF is based in Washington, DC, and includes an advisory board comprising leading figures from industry, academia, law, and advocacy groups.

Support for this program was provided by the Robert Wood Johnson Foundation.
The views expressed here do not necessarily reflect the views of the Foundation.

1400 EYE STREET NW | SUITE 450 | WASHINGTON, DC 20005 INFO@FPF.ORG | 202-768-8950