FUTURE OF PRIVACY FORUM

JULY 2021

DIGITAL CONTACT TRACING TECHNOLOGY

Privacy and Equity Principles and Framework

INTRODUCTION

Contact tracing has long been a manual disease tracking process used by public health authorities to monitor the spread of infectious diseases. During the COVID-19 pandemic, digital contact tracing technologies (DCTT) were developed as exposure notification tools to help safely reopen economies, workplaces, and other public and private spaces and settings.[1] Notably, DCTT consists of mobile apps and devices employing Bluetooth and/or geolocation features intended to provide rapid and real-time virus exposure notifications to users.

Experts expect DCTT efforts for COVID-19 to continue for some time, and for DCTT technologies and governance to evolve as public health officials lay the groundwork for DCTT programs to address new, emerging pandemic threats. In tandem, evidence continues to emerge on the efficacy and scientific validity of DCTT as DCTT becomes more widely used as a public and private health surveillance tool.

The Future of Privacy Forum (FPF) partnered with six leading privacy, social advocacy, and health equity organizations to analyze the privacy and equity trade-offs and risks that can accompany DCTT implementation: Dialogue on Diversity, the National Alliance Against Disparities in Patient Health (NADPH), BrightHive, and LGBT Tech. Focusing particularly on the impacts of DCTT on vulnerable populations, the group discussed particular risks, including but not limited to risks of disenfranchisement or social stigma related to race or ethnicity, class, religious affiliation, or other characteristics.

DCTT implementation efforts that minimize or fail to acknowledge the presence, role, or impact of these trade-offs and risks will undermine public trust in DCTT. Conversely, governance efforts that acknowledge, engage, and mitigate these risks can bolster public trust in digital contact tracing technologies. Policymakers, data protection experts, and organizations developing, administering, and providing DCTT technologies all have important roles to play.

EXECUTIVE SUMMARY

As part of its Privacy and Pandemics initiative, FPF worked with Dialogue on Diversity, the National Alliance Against Disparities in Patient Health (NADPH), BrightHive, and LGBT Tech to develop a set of actionable principles to support privacy and equity in DCTT implementation.

The principles advise organizations implementing DCTT to:

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

FPF and these six organizations call on DCTT developers and organizations implementing DCTT to commit to these principles.

On the following pages, we:

1. Describe each principle;
2. Summarize case scenarios that illustrate how DCTT technologies can raise data protection risks, particularly risks for vulnerable individuals, including racial and religious minorities, LGBTQ+ individuals, and immigrant communities; and
3. Highlight key definitions and other resources to inform the implementation of DCTT from a privacy and equity perspective.

ACTIONABLE PRIVACY AND EQUITY PRINCIPLES FOR DIGITAL CONTACT TRACING TECHNOLOGY

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 explicitly state when and the duration of time for which sensitive data is collected.

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.

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.

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.

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.

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.

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.

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.

To sign on to the Digital Contact Tracing Technologies Principles, contact us at info@fpf.org.

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)

REAL-WORLD CASE SCENARIOS

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

1 Examples of publicly available DCTTs include COVIDWISE, an app developed by the Virginia Department of Health (US); CO Exposure Notifications, developed by the Colorado Department of Public Health & Environment and Colorado State Emergency Operations Center (US); and an Association of Public Health Laboratories platform developed by multi-state epidemiologists and the Metropolitan Washington Council of Governments for exposure notification across neighboring state lines in the District of Columbia, Maryland, Virginia, and West Virginia (US). Examples of DCTT used outside of the US include Stopp Corona, developed by the Austria Federal Ministry of Health and Coronavirus – SUS, developed by the Brazil federal government.

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