MIT Computational Law Report

Digital Contact Tracing: A Playbook for Responsible Data Use

Kelsey Finch, Maithri Vangala, Sara Jordan, Natalie Ortiz, Rachele Hendricks-Sturrup, Samantha Levy, Pollyanna Sanderson, Hana Passen, Brian Lim, Brenda Leong, Katelyn Ringrose, Autumn Felty, Joanna Tess, Kelly Dolan, Natalie Evans Harris, Matt Gee

Published on: Aug 14, 2020

License: Creative Commons Attribution 4.0 International License (CC-BY 4.0)

> *This playbook was collaboratively developed by BrightHive and the Future of Privacy Forum. The original version of the playbook appeared here. For more information about BrightHive, click here; for more information about Future of Privacy Forum, click here.*

Pt. 1: Background and Overview

As the pandemic threatens the health and economic security of communities around the globe, the issue of equity—whether gender equity, equity in access, racial equity, equity for linguistic and cultural groups, and age-group equity—has come to the forefront of debates among policymakers, civil society, educators, industry leaders, and other stakeholders. For groups invested in addressing the pandemic through uses of digital contact tracing technologies (DCTT), the threat that DCTT could exacerbate the social inequities should be acknowledged and taken seriously. Likewise, moving privacy and equity to the center of the conversation about DCTT can improve trust in the institutions administering DCTT and contribute to better local adoption.

In this brief discussion, we outline considerations in equity and fairness to encourage those using this playbook to think about how DCTT can use in a trusted, service-integrated, and nondiscriminatory way and, subsequently, improve adoption. We also highlight emerging legislative trends shaping DCTT initiatives across the US, which are increasingly codifying the equitable and ethical considerations raised in this Playbook.

Privacy, Equity, and COVID-19

While privacy and equity may not be the first thing people think about when discussing how to combat COVID-19, each is foundational in effectively addressing the challenges caused by the virus. Addressing COVID-19 requires all members of a community to work together and trust in the institutions implementing digital solutions for COVID-19.

The COVID-19 pandemic has drawn greater attention toward numerous societal disparities, including access to technology, health information, and healthcare. Management and tracking of COVID-19 infections can undoubtedly amplify existing inequities, whether this is through manual contact tracing or DCTT that relies on diagnostic testing for results. Moreover, digital management of COVID-19 depends on distribution of associated infrastructure, such as broadband access, ownership and use of smartphones, and even electricity. Public health research has shown that COVID-19 infections have disproportionately impacted different groups of people throughout America. Senior citizens succumb to infections at a higher rate, and senior citizens of color are at an even higher risk of premature death. Among younger persons, infection rates, morbidity, and mortality affect low income essential workers tasked with maintaining our functioning economy at higher rates than others of the same age

or socioeconomic status. Without a critical amount of support within a community, the ability to effectively conduct contact tracing goes down.

Additionally, there are communities throughout the United States that are over-policed and over-surveilled. This is important because without institutional trust in the entities administering DCTT, many will see the risk posed by over-policing and over-surveilling as not being worth the benefit of effective contact tracing. This is particularly true in communities with large immigrant populations who may be without documentation or with language barriers. As a fundamental principle for use and design, no contact tracing technology should be developed or deployed if it will exacerbate existing inequalities or create new pathways for the inequitable treatment of persons or communities. In particular, DCTT should not elicit fear of being tracked, deported, disenfranchised, displaced, or stigmatized.

What steps can be taken to address and mitigate those inequities and leverage opportunities to foster trust among our most socially vulnerable communities? In short, a maximin principle of distribution should be embraced to maximize the minimum payoff for participation in DCTT for those most severely affected by the COVID-19 pandemic. In providing access to contact tracing technologies to the greatest number of individuals, and making purposeful steps to include those who are most negatively affected by the digital divide, the positive health effects of DCTT won't remain with those individuals who are already at low risk of contracting COVID. Also, and importantly, no DCTT user should be penalized or stigmatized in any way for any behavioral data collected and/or reported through a DCTT initiative. While these steps are larger than any one stakeholder can take alone, DCTT developers and promoters should band together to move forward on these steps in earnest.

Privacy Legislation and COVID-19

The risk that structural inequities and regulatory gaps will undermine public trust and adoption of DCTT has also spurred a new spate of state and federal legislative activity. Currently, the United States does not have a comprehensive federal privacy law, instead relying on a patchwork of state privacy laws. The absence of a comprehensive regulatory framework has left open questions about how public and private sector organizations should protect and use personal data during the COVID-19 pandemic. In an attempt to set ethical guardrails and create more clarity, legislators have introduced numerous bills to regulate contact tracing apps and COVID-19-related data.

At the federal level, there have been multiple calls for a comprehensive federal contact tracing strategy, and three key privacy bills have emerged. The Exposure Notification Privacy Act, a bipartisan bill, would apply to the operators of contact tracing apps. Many of its provisions align with Terms of Service for the Google-Apple Exposure Notification (GAEN) API. For instance, data could only be collected and processed for the purpose of responding to COVID-19, could only be retained for a certain

period of time, and only confirmed diagnoses could be processed to trigger an exposure notification. Two other bills, one introduced by Senator Wicker and one by Senator Blumenthal, would regulate COVID-19-related data more broadly. However, these bills diverge along partisan lines around key issues, including their scope, preemptive capacity, enforcement mechanisms, and anti-discrimination and research protections. Nevertheless, there is agreement between all three of these bills on the need for contact tracing apps to be fully voluntary.

In the absence of a federal law, states are leading the way when it comes to the regulation of DCTT. California (AB89) and South Carolina (HJR5202), have already passed legislation preventing budget funds from being allocated for contact tracing apps. In South Carolina, any technologies deployed for contact tracing must also be "maintained in a decentralized manner" (e.g., case management tools, or medical monitoring tools). Kansas signed HB2016 into law in June, prohibiting state and local government entities engaged in contact tracing from using smartphone location data to "identify or track…the movement of persons" for contact tracing. Notably, depending on how this is interpreted, this law might nevertheless permit the utilization of Bluetooth signals to measure relative proximity between two individuals. Digital contact tracing bills have also arisen in New Jersey, Minnesota, Utah, and in other states.

States have also been proactive in addressing barriers to trust and equity beyond contact tracing, and in particular in acting to prevent data from being repurposed in ways that may harm individuals and marginalized communities which have frequently been the target of over-policing and surveillance. For example, the New York legislature passed a bill (A10500) with wide support from civil rights and advocacy groups to protect the confidentiality of contact tracing information and prohibit access by law enforcement and immigration authorities. A similar bill has gained traction in California (AB660). Other recent New York bills would ban all persons and state entities from collecting or using facial recognition technology to track COVID-19 (S8311) or impose obligations around transparency, data minimization, purpose limitations, data retention, and data security on government entities that collect, use, or disclose "emergency health data" (e.g., location, proximity, and health-related data), entities that develop or operate COVID-related apps, and downstream third party recipients (S8448). Similar to a bill in California (AB1782), New York's S8448 would also aim to empower individuals to revoke their consent to the collection, use, and sharing of their personal information.

While the relationship between DCTT, privacy, and equity during the COVID-19 pandemic is a complex one, it is more important than ever to ensure individuals and communities are protected and their personal information is used in an ethical and responsible manner.

Introduction

COVID-19 is an unprecedented public health crisis. As the disease continues to spread through communities across the U.S. and abroad, information about the illness continues to evolve. To slow the spread, public health officials are turning to contact tracing as a means to track cases, identify sources of transmission, and inform people who may have been exposed to take precautions that can prevent further transmission.

Manual contact tracing is a scientifically established method that can help understand the spread of communicable diseases. For contact tracing to be most effective, people must share sensitive personal information regarding their whereabouts and the people with whom they have been in close proximity. This information allows contact tracing professionals to trace or map their locations and connect with those with whom they have been in close contact. One unique feature of the COVID-19 era is the way digital technology is facilitating these processes.

Digital contact tracing technology (DCTT) has the potential to significantly reduce the spread of COVID-19 and assist with reopening efforts. Technologies such as smartphones, mobile device applications (apps), and the network of data transfer protocols (e.g., APIs) have been pulled together to produce digital contact tracing technologies. Contact tracing apps track an individual's exposure to COVID-19 and notify the individual if they encounter another app user who has tested positive for the virus, or who has self-reported as positive. These apps typically track users through either geolocation data or Bluetooth proximity data, or both.

Apps relying on geolocation data use GPS, WiFi, or cell phone towers to track users' locations, while Bluetooth apps check for other nearby devices using the app and exchange a unique, often rotating, token with the other device.[1] The app later searches a database of tokens registered to users who have self-reported testing positive for COVID-19 to determine if the user was exposed to the virus.[2]

Apps using geolocation data are considered more privacy invasive because they rely on tracking the user's location to determine proximity to other users. Bluetooth proximity apps only collect proximity data but rely on constant broadcast from a Bluetooth device, and may be less accurate than apps relying on location data.[3] This is a particular problem for centralized Bluetooth-based apps, which are not able to make use of the Google-Apple Exposure Notification API for decentralized exposure notification apps.

The design and use of these apps create privacy risks and raise ethical questions. *MIT Technology Review* assessed apps developed by 25 countries, while the Internet Digital Accountability Council reviewed 108 apps across 41 countries. Many of these apps failed to minimize their collection efforts and did not provide guarantees for destroying the data after a set period. Some countries' apps also

failed to place limits on the use of collected data and many of the apps reviewed did not provide transparency around their policies or design.[4] By taking these concerns into account, organizations that develop or use contact tracing apps can protect both health and privacy, and increase trust in contact tracing apps and other digital tools.

While health behavior changes at the population level, such as social distancing, hand washing, and wearing face coverings, are the current best approach to containing the spread of COVID-19, both analog and digital contact tracing are important elements of a comprehensive approach to containing the spread of this viral disease. Nevertheless, DCTT raises significant ethical and privacy concerns that should be addressed through design and policy.

Public health authorities, application developers, and users of DCTT need better information on how to best preserve privacy and ensure ethical use of contact tracing data, so they can better scale contact tracing initiatives and reduce the spread of COVID-19.

BrightHive and the Future of Privacy Forum teamed up to develop this privacy playbook to assist the coalitions of professionals invested in development and deployment of trusted DCTT. The playbook provides a series of actionable steps that purposefully address the privacy concerns of DCTT and support the development of ethical and responsible digital contact tracing protocols.

In particular, this playbook has been developed with the following types of scenarios, or use cases, in mind: 1) easing tension between application providers, public health officials, and government authorities; 2) supporting "opt-in" models for individuals to share health and location data; 3) supporting employers that are turning to internal contact tracing when their workplaces reopen.

This playbook is organized into two categories: Foundational and organizational plays, and technical and operational plays. Foundational and organizational plays create a strong, diverse coalition with a unified goal and set of values, aid in the administration of DCTT initiatives, and ensure that the coalition adheres to its shared values and gains the public's trust. These plays are geared toward leadership, policy, and partnership roles in an initiative.

The technical and operational plays support implementing the DCTT initiative in a way that is consistent with other plays, the coalition's values, and users' privacy rights. These plays are geared toward technical, project management, and day-to-day operational roles in the initiative.

While plays are geared toward different roles, BrightHive and FPF advise collaborating across team and function through the lifecycle of the DCTT initiative.

Opportunities to Collaborate

- Suggest a play to add to this playbook or suggest edits by sending us a message.

- Discuss this playbook and share learnings with others using the playbook in our BrightHive Responsible Data Sharing Slack Community.

Resources

This playbook was informed by the following resources: insights and recommendations from FPF workshops, publications & testimony; Georgetown Beeck Center Data Governance Handbook; Johns Hopkins Digital Contact Tracing book; law.MIT.edu privacy principles and related efforts; STAT news articles and commentary; and other data protection COVID-19 guidance/resources.

Acknowledgements

BrightHive would like to thank Kelly Dolan, Autumn Felty, Matt Gee, Natalie Evans Harris, Samantha Levy, Brian Lim, Natalie Ortiz, Hana Passen, Joanna Tess, and Maithri Vangala for their expertise and contributions to the development of this playbook.

Future of Privacy Forum would like to thank Kelsey Finch, Dr. Sara Jordan, Brenda Leong, Katelyn Ringrose, Pollyanna Sanderson, and Dr. Rachele Hendricks-Sturrup for their expertise and contributions to the development of this playbook.

Pt. 2: Playbook for Responsible Data Use

Foundational and Organizational Plays to Build a Coalition to Support a DCTT Initiative

1. Follow the lead of public health experts and use evidence-based solutions

It is essential that members of a DCTT initiative coalition work with medical and public health partners to understand their data needs. Decisions about which data, analytic, and technological models to pursue should be based on medical and public health partners' needs, their estimates of efficacy, and should be grounded in the best available evidence.

Checklist

[ ] Ensure DCTT uses and limitations have been taken into account, documented, and mitigated where appropriate, before implementation.

[ ] Continuously monitor the state of DCTT performance across various contexts, including monitoring for new research or evidence, alternative technologies, or unintended consequences (such as negative impacts on public health goals or unfair advantages or disadvantages for certain communities).

[ ] Commit to limiting the scope of the DCTT initiative according to the advice of public health experts, including policies for dissolution of activities that:

[ ] Prove to be poorly validated or ineffective by epidemiologist or expert assessment for controlling the pandemic or infection chains, or

[ ] Exceed the scope of its intended public health purpose to reduce the transmission of COVID-19.

Key Questions

- Has the DCTT implementation been assessed by epidemiological experts? Has it been assessed against generally acceptable contact tracing privacy standards and principles?
- How have limitations to DCTT been identified and addressed (including limitations related to accuracy, relevance, power, and interoperability with epidemiological models)?
- How will the DCTT system's performance be monitored and evaluated?
- What is the process to modify or terminate DCTT activities if they are found to be ineffective or at risk of exceeding their original scope?

2. Decision-makers should be guided by necessity, proportionality, and purpose limitations

Measures taken in response to pandemics should be necessary and proportionate, to ensure that responses will be beneficial to solving the crisis without undue infringement on individual privacy and civil rights. Any personal information collected and used to control the harmful effects and spread of a pandemic should be strictly time-limited and confined to a specific, well-defined public health purpose. Historical evidence suggests that it is difficult to discontinue practices initiated during an emergency, and that proactive measures are required to avoid "mission creep." Coalitions seeking to use personal information to control the harmful effects and spread of a pandemic should ask themselves whether or not a specific measure constitutes a necessary, appropriate, and proportionate action within a democratic society.

Checklist

[ ] Establish an exit strategy up front to protect against continued "emergency practices" after the end of the public health crisis.

[ ] Proactively identify and mitigate risks of mission creep and new or unanticipated uses of personal information.

[ ] Deploy DCTT in the least intrusive way and handle personal information at the lowest level of identifiability and scale necessary to accomplish stated public health goals.

[ ] Clearly articulate the specific risks and benefits to individuals and the public that are created by the DCTT.

[ ] Collect only the personal information strictly necessary to accomplish stated public health goals and nothing more.

Key Questions

- Which medical and public health experts were consulted to determine the types of personal information necessary to accomplish specific public health goals?
- How were the anticipated impacts of the DCTT identified and weighed to ensure that potential risks to individuals and society are proportionate to the potential benefits?
- Are there components of the DCTT service for which aggregate information or summary statistics, rather than individual or identifiable information, are sufficient?
- If there are multiple options for implementing certain DCTT components or functionalities, which is the most privacy-preserving that still accomplishes stated public health goals?
- If personal data is shared with partners or service providers, are there equally strict limitations on its duration and use by other entities?
  - Who will proactively audit DCTT data systems to ensure that data is not used beyond the original purposes and stated public health goals for which it was collected?
  - How will personal information and DCTT services be safely and securely shut down when no longer needed, or when the public health emergency has ended?

3. Work with established partners who have demonstrated experience with responsible data sharing

Trusted partners with the organizational and technical capacity to support DCTTs are essential. Some organizations, such as those with established 'Data for Good' programs, may already have experience sharing data in privacy-protecting ways with university, NGO, or government partners, including public health authorities. In addition, university-based programs and services, including research centers with experience in data ethics, might streamline the establishment of trusted data sharing arrangements between public agencies, companies developing and/or providing DCTT, and other institutions that will need to share data with one another to coordinate contact tracing.

Checklist

[ ] Carefully select partners and service providers based on their experience safeguarding personal health information and established reputation in the health sector.

[ ] Have all partners and service providers commit to accountability and transparency, and provide timely communication to communities and stakeholders.

[ ] Agree to terms and data uses with partners and service providers in advance, before any personal data is collected.

[ ] Develop guidelines to define roles and responsibilities for partners and service providers in the DCTT initiative, as applicable.

Key Questions

- Do all parties that will handle DCTT data have a demonstrated history of safeguarding sensitive health information? How is it demonstrated?
- Do all project partners have evidence of a commitment to protecting individual privacy?
- Are there clear contractual agreements in place describing the roles and responsibilities of each partner, particularly with regards to their handling and use of personal data?
- What is the process, and who is responsible, for conducting due diligence on all partners and service providers?
- What is the process to vet and audit service providers' privacy and security practices, and who is responsible for overseeing the process?

4. Develop a data governance structure

At the outset of a DCT development project, establish a governance committee including partners, experts, data users, and DCTT users who will guide development of processes and procedures for collection, use, and destruction of data. This group should include a diverse array of individuals representing state and local public health agencies, privacy advocates, organizations that have the legitimacy to represent the individuals who are being asked to share their contact data, and other types of community advocacy organizations that want to support public health efforts while being responsive to ethical concerns. Do not wait until the technology solution is determined or implemented to establish and convene this committee.

Checklist

[ ] Create a steering committee that represents the array of data stakeholders in the DCTT initiative, including those that provide and use contact tracing data.

[ ] Establish a charter or similar covenant that clearly defines roles and responsibilities, and enumerates the privacy and ethical principles that guide the committee's work and decisions about data use.

[ ] Define the boundaries of the digital contact tracing initiative to prevent mission creep and deter potential secondary uses of personal data that are tangential to the immediate goals and/or use cases that do not align with the values and ethical principles articulated by the steering committee.

[ ] Use the committee to inform the development of consent and data sharing protocols and processes.

Key Questions

- Does the committee agree on a clearly defined goal for the use of DCTT and a definition of success? If not, is there a process for issue escalation? Who would have final decision-making authority in cases when the committee disagrees?
- Are the ways that data may be collected and will be shared clear to every individual and organization on the committee?
- Does the group represent people whose data is being collected and used and whose privacy at risk?
- Is each individual and organization on the committee committed to upholding the privacy and ethical principles it has articulated as core to contact tracing data sharing?

5. Go the extra mile to seek public trust

While transparency on its own is insufficient to protect individual privacy, respect for individual autonomy requires that the public understand how personal data is used and protected from misuse during a health crisis. Certain public health measures, including DCTT, rely on individuals' willingness to provide their information in service of a larger goal. In support of such measures, governments, public health authorities, and corporate leaders seeking to share data should take extra steps to engage the public and be transparent about how personal data is used, by whom, and for what specific purposes.

Checklist

[ ] Give the public complete and easy-to-understand descriptions of how personal information is handled and safeguarded.

[ ] Clearly and publicly identify any government authorities, companies, institutions, or other entities that handle personal information collected as part of a DCTT initiative. Make available, upon reasonable request, the roles or officials involved in the initiative.

[ ] Provide a clear legal basis for the collection of personal information as appropriate.

[ ] Describe how the use of personal information will be limited, including prohibited uses and users.

[ ] Regularly update the public about how effective the DCTT initiative is, the extent to which public health goals are achieved, and highlight any unintended consequences observed.

[ ] Require valid legal process, such as a court order, for law enforcement or other government officials access to centralized DCTT user data, and publish regular transparency reports documenting such requests.

Key Questions

- Outside of a legal privacy notice, how does the initiative intend to communicate in plain language with individual users and the public about its performance and important privacy updates?
- Does the DCTT initiative's privacy notice meet legal and industry best practices?
- Is there a specific legal basis for the initiative's collection and processing of personal information for public health purposes? If so, is it time-limited, such as for the duration of a declared public health emergency?
- How will all partners and service providers that will handle personal data as part of the initiative be identified to the public, and how will this information be kept up to date?
- Are key technical components and essential data-handling principles or guidelines for the initiative available for independent or public review?
- Are transparency reports about law enforcement or other government requests for access to DCTT data clear, accessible, and timely?
- Based on the DCTT design, what legal process is considered by courts sufficient for law enforcement to gain access to the data? Is a subpoena or lower standard sufficient, or is a warrant required?

6. Respect context

Meaningful and inclusive public engagement is essential to building health tools and analytics that reflect generally-held collective values, including privacy, equity, efficiency, community health, and more. If deployed un-critically, digital health technologies risk exacerbating existing societal inequalities, including racial, socioeconomic, and digital divides. Coalitions that seek to deploy a DCTT iniatitive should recognize and address such concerns, and ensure that these technologies do not subject communities to additional discrimination or unfairness.

Checklist

[ ] Create opportunities for inclusive and meaningful public engagement at every stage in the project development lifecycle, and use what is learned during those engagements to design and implement initiatives that align with and reflect the community's values.

[ ] Identify and address barriers that vulnerable or minority communities face in accessing digital tools and resources, including limited access to health care or digital services, and work to rectify them.

[ ] Deploy DCTT as part of a broader strategy that ensures individuals without access to digital technologies or services are not left behind, and that does not reinforce existing biases or unfair disadvantages across communities.

[ ] Recognize and account for the diversity of values held by individual members of society, as well as differing risk tolerances and privacy preferences.

Key Questions

- Has the initiative regularly and meaningfully engaged community stakeholders to understand their feedback, opinions, and concerns? What do community stakeholders say about about whether or how DCTT might subject them or others to possible discrimination or disadvantage?
- Are the initiative's public engagements building relationships and trust with community stakeholders?
- What steps are being taken to ensure that the technology design reflects an appropriate balance and prioritization of the identified community values?
- What steps are being taken to understand--and prevent--DCTT from being used in ways that are potentially overreaching or harmful, such as contributing to public or private surveillance for non-public health purposes?
- What strategies have been identified to leverage the DCTT initiative in ways that intentionally address or rectify existing inequities?

7. Individual data sharing must be voluntary

Governments should not require individuals to share personal health information or mandate the use of digital contact training technologies. Any incentives provided to encourage the adoption of such technologies must not be coercive, but rather support their equitable and voluntary use.

Checklist

[ ] Get affirmative, informed consent from individuals before collecting any personal information and before making any material changes to how personal information is handled.

[ ] Develop a consent flow that is appropriate to the situation and individual.

[ ] Provide individuals or their legally authorized representatives with a way to withdraw their consent.

[ ] Do not provide incentives that are coercive or would encourage inequitable outcomes.

[ ] Do not bundle consent to DCTT with other functionalities.

Key Questions

- Are individuals provided with easy-to-understand information about how their data will be collected, used, shared, stored, and safeguarded before being asked to consent to the collection of their personal information?
- Is the consent provided freely given, specific, informed, and unambiguous?
- Is it as easy for individuals to withdraw consent as it was to provide it?

- Could any incentives provided to encourage DCTT services be considered coercive, inequitable, exploitive, or not aligned with effective use of the technology?
- How is your consent flow consistent with the context and organizational best practices? (E.g., standards for informed consent from public health authorities, from humanitarian experts, privacy regulators, or from human-centered design experts).
- Are there features for individuals to provide more (or less) personal information if it is their preference?
- What is the process for asking individuals to re-consent to sharing their data for purposes outside the original scope of limiting the spread of COVID-19?

8. Design accessible features

In a public health crisis, the reliability and representativeness of DCTT information is vitally important. However, digital technologies and services are not always designed in ways that are accessible to individuals with disabilities and may fail to adequately record their experiences. The consequences of this sort of biased or inaccurate data can be lasting, leading to poor or inefficient decision-making, unethical or illegal data uses, or discriminatory outcomes. DCTT initiatives and features should be designed in ways that are accessible to all.

Checklist

[ ] Design all DCTT initiative services to be fully accessible and based on the latest World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) standards.

[ ] Support interoperability with the widest array of accessibility functions on major mobile devices possible.

[ ] Explicitly recognize and rectify any remaining accessibility gaps that may limit persons with disabilities from participating in the DCTT initiative, to the extent possible.

Key Questions

- Have people with disabilities or legitimate representatives of their community been consulted for advice on design of DCTT features?
- Have benchmarks and standards for accessibility been consulted throughout the design process?
- Has the DCTT initiative designed a service that accounts for changes in individuals' abilities related to their potential illness trajectory?

9. Hold decision-makers accountable

In order to maintain public trust and legitimacy, oversight and accountability mechanisms must be clear and functional at every stage in the process. Systems used to support a DCTT initiative must be

continuously maintained and monitored to ensure that they are effective, that they are not causing harm, and that they are not imposing disparate impacts across communities. It is also essential that data protections be enforced, and that organizations create mechanisms for individuals and experts to raise concerns and ask questions.

Checklist

[ ] Put public authorities in the driver's seat, and ensure that leadership of the DCTT initiative includes public officials who are accountable to the public through appropriate electoral or appointment mechanisms.

[ ] Provide individuals and diverse communities with meaningful opportunities to contribute to the design and oversight of the DCTT initiative.

[ ] Designate a senior leader to be responsible for day-to-day privacy and data protection activities.

[ ] Conduct regular reviews and audits of data-handling procedures to ensure that personal information is being used and safeguarded as promised.

[ ] Establish mechanisms to escalate serious privacy or security concerns to initiative leaders, such as the steering committee.

[ ] Create a mechanism for external researchers and experts to report privacy or security vulnerabilities.

[ ] Create accessible public platforms for individuals to ask general and technical questions, file complaints, learn more, and contribute to the DCTT initiative.

Key Questions

- Which public authorities or officials are overseeing the DCTT initiative's efforts? Have such authorities provided any specific guidance or resources for safeguarding DCTT data?
- Are there independent auditors or experts who can assess the initiative's compliance with data protection and data security best practices?
- How will the DCTT initiative measure the success of its oversight and accountability mechanisms?
- Will the initiative provide a monitored, open, accessible channel to the public (such as conversational wizards or 211/ 311/811 community lines)?

Technical & Operational Plays to Inform the Lifecycle of DCTT Systems

10. Keep systems secure

Centralized repositories of data can elevate privacy and security risks and attract unauthorized attempts to access or use personal information. DCTT initiatives must keep data secure against both internal and external threats. Robust technical controls such as encryption and access limitations, along with regular security audits and vulnerability tests, are essential safeguards.

Checklist

[ ] Develop and document a comprehensive data security program that ensures DCTT data is protected from unauthorized access or use at every point in its lifecycle, from collection to destruction or storage, including backups.

[ ] Proactively monitor and test the DCTT initiative's systems for security vulnerabilities.

[ ] Limit access to personal information through technical, legal, and organizational controls.

[ ] Monitor and log all access to and handling of personal information, including by partners and service providers.

[ ] Create common security protocols for each unit when federated data architectures are used.

[ ] Encrypt personal data in transit and at rest, to the extent possible, using proven cryptographic techniques.

Key Questions

- Are strong and legally compliant computer-based security systems being used to protect against internal and external security breaches or unauthorized access and use of personal data?
- In the event that there is a security incident or breach, who is responsible for rectifying the situation and notifying impacted individuals?
- Is access to users' personal data limited to only the minimum necessary initiative employees to protect against internal threats or misuses of data?
- Are personal data securely stored on individual and organizational devices and not publicly available?

11. Support dynamic and interoperable systems

Because public health emergencies involving communicable diseases are quickly evolving, coalitions supporting DCTT initiatives must ensure that the data produced is equally dynamic. Initiatives and the data and systems they rely on must be able to adapt to changing medical, legal, social, and technical factors. Data collected in response to a crisis such as a pandemic disease is typically needed by multiple

types of organizations in numerous jurisdictions, and interoperability between digital systems is essential to ensuring collected information is able to serve its intended purpose.

Checklist

[ ] Communicate with partners and service providers to design DCTT systems' data structures for the greatest extent of interoperability possible.

[ ] Continuously monitor and evaluate whether the DCTT's technical design is appropriate and responsive to the current public health situation.

[ ] Embed privacy by design principles across the lifecycle of DCTT.

[ ] Follow or establish common standards for data protection, preservation, and quality among the initiative's partners and service providers.

[ ] Agree on a common protocol and compatible data structures to ensure minimum necessary exchange and processing of data.

Key Questions

- Which organizations are a priority for the initiative to coordinate with, in order to minimize duplication of efforts and data collection?
- How will the initiative ensure that it can support a dynamic DCTT design that is responsive to evolving public health needs without leading to increased or unanticipated data collection, secondary uses, or mission creep?
- Have data interoperability structures, such as common ontologies, meta-data descriptions, and data dictionaries been consulted? Have these interoperability structures been checked for conformity to expert standards in the medical or public health profession?
- How does the DCTT initiative support the tracing of contacts across physical and jurisdictional borders, in both a technical and organizational manner?

12. Conduct privacy risk assessments

When responsible organizations identify new ways to collect or use personal data, they utilize privacy impact assessments (PIAs) to systematically identify and address potential privacy issues. Given the volume and sensitivity of personal information required for effective pandemic response, including information related to health status, location and mobility, and employment, DCTT initiatives must proactively identify, document, and mitigate potential privacy risks. Best practices, frameworks, and tools for conducting privacy and data protection impact assessments are well-established in both the public and private sectors.

Checklist

[ ] Conduct a PIA as early as possible, before the DCTT initiative collects or handles any personal information.

[ ] Document any potential privacy risks identified by the PIA and how they will be addressed or mitigated by the initiative, including its partners and service providers.

[ ] Complement a privacy risk assessment with a data benefit assessment, so that the benefits and risks to individuals, communities, and society as a whole can be considered holistically.

[ ] Articulate any countervailing policies or factors that justify accepting whatever residual privacy risks remain.

[ ] Publish privacy risk and benefit assessments for public review.

[ ] Review PIAs on a regular basis, and update them whenever there is a material change in how personal information is handled.

Key Questions

- Who within the DCTT initiative will be responsible for conducting PIAs and where will it be stored?
- Will there be an opportunity for individuals or community stakeholders to participate in the PIA process, such as by helping identify unintended consequences?
- Is there a mechanism in place to trigger re-review of the initiative (e.g., when there has been a material change to the way data is collected or used, semi-annually, etc.)?
- Will the final risk assessment be made available to the public?

13. Support individual controls and choices

Individuals who choose to adopt digital contact tracing technologies should have their privacy and data protected by design and by default. To the extent possible, individuals should be able to make meaningful choices about how, with whom, and for what purposes their personal information is shared, as well as an ability to change their mind. Users should be able to view, correct, or request the deletion of their personal data, to the extent possible.

Checklist

[ ] Let individuals see and access the personal data that the DCTT initiative, including partners and service providers, holds about them.

[ ] Give individuals a way to make corrections to the personal data that the DCTT initiative holds about them.

[ ] Allow individuals to delete or request the deletion of their personal data, to the extent possible.

[ ] Provide individuals with portable, machine-readable copies of their personal information that the individual can transfer to another service if they desire.

[ ] Allow individuals to request human review of any automated decision-making that would have a legal or similarly significant effect.

Key Questions

- How does the DCTT initiative allow individuals to access, correct, delete, or port their personal information? Are such capabilities provided at no charge and in a timely manner?
- What transparency and review mechanisms are in place for situations where the initiative is not able to reasonably provide individuals with mechanisms to access, correct, delete, or port their personal information?
- Will the DCTT initiative incorporate automated decision-making processes that could have legal or similarly significant effects for individuals? If so, who will be responsible for reviewing those decisions on behalf of impacted individuals?

14. Apply privacy enhancing technologies (PETs)

Public health initiatives collecting and handling personal information should adopt advanced privacy-preserving and privacy-enhancing technologies from the outset. Sophisticated approaches such as differential privacy or secure multiparty computation should be considered where practical, and technical measures should be complemented with organizational and legal controls. DCTT initiatives should incorporate the most robust privacy-enhancing technologies appropriate given analytic and public health needs, and the techniques and methodologies applied should be published publicly to enable independent review.

Checklist

[ ] Incorporate privacy and data protection checks at each stage of the software development lifecycle.

[ ] Test systems before deployment with and without incorporation of privacy enhancing technologies to identify areas of greater data leak or data exposure.

[ ] Interface often with security and design teams to ensure software architecture choices do not inadvertently undermine incorporation of privacy enhancing technologies.

[ ] Publish your technical documentation and methodology so that it is available for public review.

Key Questions

- Have technical and design teams been actively encouraged to incorporate privacy enhancing technologies throughout the design process?
- Which data minimization practices have been considered and applied?
- Will data be released publicly (where it can be subjected to a wide array of potential re-identification attacks) or used and shared only subject to legal and organizational controls?
- How will the initiative determine the appropriate level of aggregation or perturbation of the personal information that it handles to preserve privacy and maintain data utility?
- Are formal or cryptographically guaranteed privacy enhancing technologies appropriate for any of the initiative's use cases?
- Are there independent auditors or experts who can assess the initiative's application of privacy-enhancing technologies?

15. Prepare DCTT users for possible uses of data in Artificial Intelligence (AI) and Machine Learning (ML)

Machine learning-based technologies can play a substantial role in this pandemic and future public health response measures. Experts can use machine learning to study the virus, test potential treatments, diagnose individuals, analyze the public health impacts, and more. Digital contact tracing data will provide valuable information from which such systems can draw insights into individual and group behavior. When coalitions support DCTT initiatives that expect data will be used in AI or ML research or development, additional data protection precautions must be taken.

Checklist

[ ] Monitor DCTT systems that use ML (e.g., to optimize individuals' experiences or improve functionality of exposure notifications) for performance and model drift.

[ ] Utilize privacy-preserving ML techniques, such as federated ML, and monitor them on an ongoing basis to ensure that privacy is maintained.

[ ] Conduct extensive audits of ML systems during development, testing, and deployment.

[ ] Design stakeholder values into ML systems, where technically feasible.

[ ] Conduct differential impact assessments on 'intermediate models' of DCTT systems using ML, in order to test whether they create discriminatory impacts.

Key Questions

- Will DCTT data in this initiative be used for training, testing, or validating AI/ ML systems? What about by partners or service providers?
- Are third party software development kits (SDKs) that include uses of AI or ML incorporated into the DCTT? Do those SDKs have access to all of the data within the DCTT?
- Have potential AI/ML uses of DCTT data been tested against privacy-preserved data sets, such as simulated data or digital twins?
- Have any differential impacts, unacceptable data leaks, or related privacy concerns identified a consequence of those tests been mitigated or addressed?

16. Delete or de-identify after the public health emergency

DCTT data processed in response to the crisis should be kept only for the duration of the public health emergency. Once appropriate authorities have determined that the crisis has ended, personal information should be promptly deleted or permanently de-identified. In certain cases, it may be appropriate for *non-identifiable* information to be kept for limited, public-interest historical and research purposes, subject to appropriate ethical safeguards and controls.

Checklist

[ ] Promptly de-identify any remaining personal information after the public health emergency, using robust technical, organizational, and legal safeguards appropriate to the circumstances *(see Play 14: Privacy Enhancing Technologies)*.

[ ] Promptly and securely dispose of any remaining personal information after the public health emergency, both physically and electronically.

[ ] Communicate with the scientific community early in the initiative's development process to determine which forms of data should be considered an important part of future scientific research.

[ ] Give individuals opportunities to opt-in to public-interest historical and research use of their personal information, where appropriate.

Key Questions

- How much time after the official end of the public health emergency will the initiative require to securely delete or de-identify all remaining personal information?
- Have public health researchers been consulted for their data needs when developing processes and procedures for data preservation, aggregation or de-identification, and deletion?
- Are there mechanisms in place to evaluate the integrity, ethics, and lawfulness of any proposed secondary uses of de-identified DCTT data? *(See Play 17: Ethical Review)*

- If de-identified data is maintained for limited, public-interest historical and research purposes, what policies and procedures are in place to prevent or significantly reduce the probability of re-identification or incompatible secondary use?
- Are there independent auditors or experts who can validate that the initiative has securely deleted or de-identified all remaining personal information and does not retain any identifiable DCTT data after the end of the public health emergency?

17. Seek independent ethical review

Given both the significant benefits to society and the significant privacy risks to individuals of DCTT, it is essential that DCTT initiatives are held to the highest standards of ethical governance and digital design. Ethical reviews are also important for determining which secondary uses of DCTT data, such as public interest or historical research, are appropriate. Such review processes could consist of several components, such as review by an internal committee, an external committee, or a body of collaborative stakeholders. Ethical standards appropriate to DCTT initiatives should be defined by the groups producing or impacted by the technology.

Checklist

[ ] Establish an ethical review process to assess the privacy risks arising from collecting, sharing, combining, using, and/or preserving DCTT data.

[ ] Require ethical review and ongoing oversight for any new or materially changed data collection practices, features, and uses.

[ ] Publish the ethical standards or frameworks that will guide ethical reviews for the initiative.

[ ] Gather experts and form an independent body or board that is not involved in the design or conduct of the DCTT initiative and that receives no monetary contribution for any intended collection or uses of the data.

[ ] Document the decisions and rationale of each ethical review conducted.

Key Questions

- What standards or frameworks will guide the ethical review process for this initiative?
- Do any of the partners to this initiative engage in ethical reviews on a regular basis, such as through an institutional review board?
- What level of independence will this initiative's ethical review process require, in order to maintain public trust?
- How diverse is the composition of the ethical review body? Does it include representatives from groups impacted by the technology?

Footnotes

1. Tokens are a unique identifier tied to a user's phone. Apps that make use of rotating tokens change the token identified with a user's phone on a regular basis. This helps protect user privacy by essentially dividing a user's data across multiple identities. ↩

2. Andy Greenberg. "How Apple and Google Are Enabling Covid-19 Contact-Tracing." *Wired*. April 10, 2020. https://www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/. ↩

3. Sam Biddle. "The Inventors of Bluetooth Say There Could Be Problems Using Their Tech for Coronavirus Contact Tracing." *The Intercept*. May 5, 2020. https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing/ ↩

4. Patrick Howell O'Neill, Tate Ryan-Mosley, & Bobbie Johnson. "A flood of coronavirus apps are tracking us. Now it's time to keep track of them." *MIT Technology Review*. May 7, 2020. ↩