TECHNOLOGIES OF PANDEMIC CONTROL //

Privacy and Ethics for COVID-19 Surveillance

S.E. Freeman

October 2020

CITRIS AND THE BANATAO INSTITUTE
CITRIS POLICY LAB
HUMAN RIGHTS CENTER
UC Berkeley School of Law

Technologies of Pandemic Control //

Privacy and Ethics for COVID-19 Surveillance

S.E. Freeman

October 2020

Contents

Executive Summary

In response to the rapid spread of COVID-19 and its devastating effect on communities across the United States, private companies, state and local governments, nonprofits, and epidemiologists have been harnessing the powers of big data and technology in an attempt to better understand and contain the spread of the virus. While the power of technology could assist in mitigating this unprecedented public health crisis, it does so at the risk of eroding significant data privacy protections and civil liberties, as well as exacerbating the structural disparities already laid bare by the pandemic itself.

Through an analysis of four technologies aimed at mitigating COVID-19 in the U.S.—exposure notification and digital proximity tracing tools, aggregated location data, symptom-tracking applications, and immunity passports—conducted from June through August 2020, we investigate how these technologies work, the privacy and ethical questions they raise, the legislation governing their use, and their potential consequences now and for a post-pandemic future. We conclude that exposure-notification tools and immunity passports lack sufficient evidence to support their use and have a high likelihood of exacerbating, rather than counteracting, the already devastating impact of the pandemic on communities of color. While aggregated location data and symptom-tracking applications have epidemiological support for specific use cases, the limited representativeness of the data and potential for mission creep risks misleading public health interventions and increasing harm to already marginalized communities.

Given the lack of evidence for these technologies thus far and their concentration of risk on communities already hit hardest by the health and financial effects of COVID-19, we offer the following recommendations for decision-makers:

- Refocus technological skills and expertise away from interventions that lack sufficient evidence and towards existing bottlenecks in the public health and logistics infrastructure, as identified by healthcare workers and public health officials at the forefront of response efforts.

- Redirect and reinvest resources into addressing the bottlenecks identified, underfunded and under-resourced health facilities, and individuals needing financial and social support to self-isolate.

- Ensure that technological interventions are evidence-based, use verifiable data, and are driven by the public health needs of affected communities.

- Such technological interventions must be accountable to the communities using them through active collaboration, partnership, and oversight in design, implementation, and evaluation.

- Interventions, when used, should be accessible to all individuals regardless of disability or immigration status, gender identity, access to internet or housing, or other barriers to participation.

- Comprehensive federal data privacy legislation is needed, and must include strong mechanisms and resources for enforcement.

- Any user data that is collected must be subject to privacy-by-design principles, include clear limitations on purpose and use, implement post-pandemic sunsetting, and employ affirmative consent.

This report makes clear that any technological intervention must function as one component of a larger public health response, one that needs adequate resources and strong leadership to succeed. Given the dire situation in the U.S., as positive cases and death counts continue to rise in the face of weak federal leadership, partnerships between technology and public health are best placed to overcome existing obstacles to delivering equitable testing, treatment, and comprehensive care. Technology has an important role to play in facilitating a large-scale public health response, but only if attuned to, and designed to actively counteract, the racialized, gendered, and classed disparities in pandemic impact.

01 //

INTRODUCTION

01 //

INTRODUCTION

Since COVID-19 started disrupting our daily lives in early 2020, governments, public health experts, and private corporations around the world have been harnessing the powers of big data and technology in an attempt to better understand and contain the spread of the virus. In the months that followed—as shelter-in-place orders started, masks were donned, and case counts rose around the world—so did the number of technological interventions, from AI-driven policy predictions in Canada to color-coded QR codes indicating health status and mobility restrictions in China.[1]

While the incredible power of technology could pose great promise to stymie this unprecedented public health crisis, it does so at the risk of eroding civil liberties, especially the right to privacy, as well as exacerbating social and economic disparities already laid bare by the pandemic itself. What we see now is a robust online debate among researchers, technologists, legal experts, and privacy advocates over what works, what doesn't, and how user privacy can be preserved in the process. While technology might serve as a life-saving resource during this state of emergency, what precedent does the use of such technology on a mass scale set, and what ethical questions does it raise for a post-pandemic future?

This report outlines the contours of this debate, including how experts are answering such questions in the United States where concerns over app development, mass mobility tracking, and aggregated data have multiplied given the dominance of Silicon Valley and the patchwork system of data privacy regulation. This report provides a roadmap of this uncertain

[1] Bill Whitaker, "Outbreak Science: Using Artificial Intelligence to track the coronavirus pandemic," CBS 60 Minutes, April 27, 2020, https://www.cbsnews.com/news/coronavirus-outbreak-computer-algorithm-artificial-intelligence/; Paul Mozur, Raymond Zhong and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," New York Times, March 1, 2020, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

landscape, collating existing research and synthesizing recommendations into a centralized resource focused on four types of technologies aimed at mitigating the spread of COVID-19 in the U.S.: exposure notification and digital proximity tracing tools designed to assist manual contact-tracing efforts, aggregated location data, symptom-tracking applications, and immunity passports.

While privacy and security questions comprise a significant portion of this report, the research also compels us to ask what a focus on individual privacy potentially obscures. The fallout of COVID-19 has put into stark relief the structural racism that has long defined access to resources, adequate healthcare, testing, and treatment in the U.S. As many of the experts featured here make clear, technology tools and comprehensive data collection are crucial components of a large-scale public health response, yet must be attuned to the larger inequitable patterns of pandemic impact in order to counteract rather than intensify them.

Methods and Scope

This report reviews primary and secondary source material (e.g., white papers, reports, existing research, and news articles), expert panels, and podcasts, alongside select interviews with technologists and privacy experts. Research was conducted from June through August 2020. The material reviewed was published either during that time frame or before, with sources and dates indicated in the footnotes. Given the limited window of research, the speed at which research on these topics is being produced, as well as the sheer number of technologies and associated commentaries, this report is far from comprehensive. Rather, it seeks to provide a snapshot of technologies debated in the U.S. for pandemic response, how they work, as well as the privacy, security, and ethical concerns they raise. The hope is that this report will serve as a guide for navigating some of the ethical questions presented by what the Ada Lovelace Institute calls the "first pandemic in an algorithmic age," as well as a foundation for future research and recommendations as the pandemic continues.[2]

Structure of the Report

The first part of the report takes each of the four types of technologies in turn, addressing the following questions for each:

[2] Carly Kind, "What will the first pandemic of the algorithmic age mean for data governance?" Ada Lovelace Institute, April 2, 2020, https://www.adalovelaceinstitute.org/what-will-the-first-pandemic-of-the-algorithmic-age-mean-for-data-governance/.

1) How do these technologies work and for whom?
2) What is their proposed purpose?
3) What privacy, security, and ethical concerns do they raise?
4) What technology and policy requirements are needed to address those concerns?

The second section of the report provides a brief overview of existing legislation relevant to these technologies, as well as data privacy regulations introduced in Congress in relation to COVID-19 and technological interventions. The last section of the report provides conclusions and a summary of recommendations. These recommendations should be read alongside existing proposals from privacy advocates, as featured in the rest of the text.

02 //

TECHNOLOGICAL INTERVENTIONS

02 //

TECHNOLOGICAL INTERVENTIONS

EXPOSURE NOTIFICATION AND DIGITAL PROXIMITY TRACING

Since the early days of the pandemic and the initial success of the “test, trace, isolate” strategy for containing the spread of the virus in South Korea, contact tracing, alongside adequate testing and the isolation of cases, was identified by U.S. public health experts as a priority intervention to be deployed on a massive scale to control the pandemic.[3] A centuries-old public health intervention already used to identify and contain other infectious diseases, such as Ebola and tuberculosis, contact tracing aims to identify individual cases, trace those who might have been exposed to that individual, and suggest testing, isolation, and quarantine accordingly. While proven effective, it is a labor-intensive and invasive endeavor (by design), requiring hours of interviews, phone calls, and detailed questioning by trained contact tracers, that would need to be scaled up enormously in the U.S. in order to reduce rates of transmission and contain the spread of the virus. Johns Hopkins initially estimated 100,000 contact tracers would be needed country-wide, while others believe up to 300,000 could be required.[4]

In response to this need, technology companies have been developing a number of tools to automate the contact tracing process for a greater

[3] Maggie Fox, “‘We need an army’: Hiring of coronavirus trackers seen as key to curbing disease spread,” STATNews, April 13, 2020, https://www.statnews.com/2020/04/13/coronavirus-health-agencies-need-army-of-contact-tracers/; Crystal Watson et al., "A National Plan to Enable Comprehensive COVID-19 Case Finding and Contact Tracing in the US," Johns Hopkins University, April 10, 2020, https://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf.

[4] Watson et al., “National Plan,” 3; Will Feuer, "Coronavirus contact tracing is ‘not going well,’ Dr. Fauci says, U.S. still needs more testing," CNBC, June 26, 2020, https://www.cnbc.com/2020/06/26/coronavirus-contact-tracing-is-not-going-well-fauci-says.html.

proportion of the population in order to facilitate efficiency at scale. The approaches to these digital contact tracing tools vary, ranging from case management tools (e.g., platforms that manage data and contacts, to be used by trained contact tracers and clinicians); to GPS location data collected on individual devices, to then be accessed by public health authorities as part of the contact tracing process; to proximity tracing and exposure notification tools (e.g., Bluetooth applications that notify an individual if they have come into contact with someone who has tested positive for COVID-19).[5] The latter comprise the focus of this section, as these technologies have garnered much attention and resources—from Silicon Valley companies, public health authorities, and leading researchers—despite the additional data still "needed to quantify the public health value of these tools."[6]

How does it work?

Proximity tracing and exposure notification tools are voluntary, opt-in applications that utilize a device's Bluetooth signal or GPS location data (or a combination of the two) to notify individuals of their potential exposure to COVID-19 based on their proximity to other users. Whereas manual contact tracing relies on a person's memory of prolonged contact in distinct locations, proximity-tracing tools detect associations rather than record absolute location so that, once notified, an app user can get tested and/or self-isolate to prevent the spread of the virus. While there are tools that utilize both GPS and Bluetooth technology, the majority rely on the latter, largely considered to be more accurate for detecting proximity and preserving privacy.[7] Some of the differences are touched on below.

[5] Researchers at Johns Hopkins divide digital contact tracing tools into "minimal, maximal, and middle-ground approaches" in their book on the topic: Jeffrey Kahn, ed., Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance (Baltimore: Johns Hopkins University Press, 2020), https://muse.jhu.edu/book/75831. This report focuses on various "minimal" approaches, with some "middle-ground" featured for comparison. See also: Jonathan Zittrain, "Digital Contact Tracing: A Primer," Berkman Klein Center for Internet and Society, July 9, 2020, video, 8:57, https://www.youtube.com/watch?v=k0tD98B4SBM.

[6] "Guidelines for the Implementation and Use of Digital Tools to Augment Traditional Contact Tracing," Centers for Disease Control and Prevention, June 16, 2020, 2, https://www.cdc.gov/coronavirus /2019-ncov/downloads/php/guidelines-digital-tools-contact-tracing.pdf.

[7] Vi Hart et al., "Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks," Edmond J. Safra Center for Ethics at Harvard University, April 3, 2020, https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf; For more on how these technologies work, see "Bluetooth Tracking and Covid-19: A Tech Primer," Privacy International, March 31, 2020, https://privacyinternational.org/explainer/3536/bluetooth-tracking- and-covid-19-tech-primer as well as Zittrain, "Digital Primer."

The most well-known of these tools is the Google and Apple partnership on an application programming interface (API). This API is a modification of iOS and Android systems to allow for device interoperability and for apps to use the device's Bluetooth technologies for proximity sensing. Google and Apple have made clear that the API is intended for use by public health officials, who would then have applications built from the API infrastructure for download by users.[8]

Exposure notification tools built on the Google / Apple API use Bluetooth low energy (BLE) technology to notify individuals of their potential exposure to COVID-19 based on their proximity to other users' devices. Whereas manual contact tracing relies on a person's memory of prolonged contact in distinct locations gleaned through in-depth interviews and phone calls by trained contact tracers, these tools detect potential exposure of the general population, measured by being within the Bluetooth range of another device for the amount of time to potentially become exposed to the virus (i.e., within six feet for more than 15 minutes). Once a user downloads an app built on this API and turns the app on, their device will continually produce anonymized keys that are broadcasted via Bluetooth beacons and exchanged with any phone that comes within sensing range. These keys change every 10-20 minutes, do not collect or provide any identifying user information, and are stored locally for approximately 14 days (the window of potential exposure) on each device. When a user receives a positive COVID-19 result, they enter a unique authorization code from the health authority into the app, which then uploads their device's log of contacts to a local database or the cloud, depending on the app's design. No identifying information is uploaded, just the device keys. User devices regularly download the keys connected to positive test results, cross-checking for potential matches (i.e., keys exchanged with devices of users who reported positive test results). When there is a match, the app sends a notification to the user with public health information regarding next steps for self-isolation and testing.[9]

The decentralized approach utilized within the Google / Apple API is considered to be the most privacy-friendly option for exposure notification because it relies only on BLE technology for proximity sensing (vs. collecting

[8] "Exposure Notifications: Using technology to help public health authorities fight COVID-19," Google, 2020, https://www.google.com/covid19/exposurenotifications/.

[9] For a thorough description and diagram of how the API works see "Privacy-safe contact tracing using Bluetooth Low Energy," Google and Apple, 2020, https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing__Using_BLE.pdf and "Contact Tracing Cryptography Specification," Google and Apple, April 2020, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ContactTracing-CryptographySpecification.pdf.

absolute location data), does not collect personally identifiable information, and stores data primarily on the device rather than in a centralized server. The success and accuracy of these interventions, however, are still questionable and rely on a high level of participation by the general public, necessitating use among up to 50-70% of the population according to some studies.[10] Notably, as of August 24, only six states are reported to be using the platform to build their own apps.[11]

While Google and Apple's API has garnered the most attention—and now serves as the infrastructure for apps such as Covid Watch[12]—similar privacy-preserving, proximity-tracing protocols are also circulating. MIT's PACT, The University of Washington's PACT (unaffiliated), the Temporary Contact Number (TCN) Protocol, and D3-PT (a global consortium of technologists, engineers, legal experts, and epidemiologists) all use and advocate for similar privacy-preserving protocols.[13] CoEpi, another leading exposure-notification app, utilizes the same BLE proximity approach, but relies on user entry of symptoms rather than proof of a positive test result to trigger exposure notification. Future versions of the app will also collect location data if a user opts in to that feature.[14]

Other applications use time-stamped and absolute location data, often in concert with BLE technology, to better identify the moment of exposure

[10] Hart et al., "Outpacing the Virus," 15; "Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown," University of Oxford, April 16, 2020, https://www.research.ox. ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

[11] Zac Hall, "Which U.S. states are using Apple's Exposure Notification API for COVID-19 contact tracing?" 9to5Mac, last modified August 24, 2020, https://9to5mac.com/2020/10/01/covid-19-exposure-notification-api-states/.

[12] See "Origin," Covid Watch, 2020, https://www.covidwatch.org/organization; Von Arx et al., "Slowing the Spread of Infectious Diseases Using Crowdsourced Data," Covid Watch, March 20, 2020, https://blog.covidwatch.org/en/covid-watch-whitepaper-using-crowdsourced-data-to-slow-virus-spread.

[13] "PACT: Private Automated Contact Tracing," MIT, 2020, https://pact.mit.edu/; Justin Chan et al., "PACT: Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing," ArXiv, May 7, 2020, https://arxiv.org/pdf/2004.03544.pdf; "About TCN," TCN Coalition, 2020, https://tcn-coalition.org/ (which emerged from Covid Watch's Contact Event Numbers protocol; Covid Watch, 2020); "DP3T - Decentralized Privacy-Preserving Proximity Tracing," DP-3T, 2020, https://github.com/DP-3T/documents. For a detailed description of the differences between each of these approaches see Chan et al., "PACT," 14-15. For an effective overview of these proximity based efforts and the concerns they raise, also see Daniel Kahn Gillmor, "Principles for Technology-Assisted Contact Tracing," ACLU, April 16, 2020, https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing.

[14] "About CoEpi" and "Frequently Asked Questions," CoEpi, 2020, https://www.coepi.org/faq/.

through GPS (what Johns Hopkins calls "middle-ground approaches" to digital contact-tracing technology[15]). MIT's SafePaths, for example, is designed to supplement the manual memory-based tracing of individual contacts by allowing the user to voluntarily grant access to their anonymized location trail to public health officials following a positive diagnosis. The location data would be stripped of identifying information and housed on an encrypted government server to mitigate potential privacy concerns.[16] North Dakota and South Dakota's Care19 Diary app also stores a user's anonymized location data on their device for future use by public health authorities, while the Care19 Alert app provides exposure notification via the Google / Apple API.[17] Utah's HealthyTogether app uses a combination of symptom, location, and Bluetooth data to facilitate contact tracing by public health officials. Use of the app is voluntary and opt-in, and has built-in retention requirements so that data are deleted when no longer needed.[18] Despite these safeguards, the proximity approach without the collection of location data is widely considered to be the more privacy-friendly option.[19]

Why use these interventions?

Technology tools might seem like an immediate way to assist in the great public health challenge the U.S. faces, with positive cases and death counts still rising in late July and early August in all but a few states.[20] This dire public health emergency, combined with the enormous economic impact the pandemic will continue to have in the absence of a vaccine, has left many wondering how the country can start re-opening the economy safely while keeping the virus contained. Designed as a way to facilitate manual

[15] Jeffrey Kahn, ed., Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance (Baltimore: Johns Hopkins University Press, 2020), 3-4, https://muse.jhu.edu/book/75831.

[16] "Project SafePaths," MIT, 2020, https://www.media.mit.edu/projects/safepaths/overview/; Ramesh Raskar et al., "Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic," MIT, March 19, 2020, https://arxiv.org/pdf/2003.08567.pdf.

[17] "Care19," North Dakota State Government, 2020, https://ndresponse.gov/covid-19-resources/care19.

[18] "Healthy Together App," Utah State Government, 2020, https://coronavirus.utah.gov/healthy-together-app/.

[19] Gilmor, "Principles"; Hart et al., "Outpacing the Virus."

[20] Griff Witte and Ben Guarino, "It's not only coronavirus cases that are rising. Now covid deaths are, too," Washington Post, July 17, 2020, https://www.washingtonpost.com/national/its-not-only-coronavirus-cases-that-are-rising-now-covid-deaths-are-too/2020/07/17/193006e8-c868-11ea-8ffe-372be8d82298_story.html; "Coronavirus in the U.S.: Latest Map and Case Count," New York Times, updated and accessed August 26, 2020, https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html.

contact-tracing efforts, these interventions aim to maximize a privacy-utility trade off—expanding the means by which an individual can be notified of potential COVID-19 exposure while keeping privacy largely protected. The use of exposure notification tools could expand the scope of contact tracing beyond personal contacts to anonymous or brief interactions to inform and protect the maximum number of people affected, and Bluetooth is seen to be more accurate than GPS-based methods with less chance of false positives.[21] In addition, the fact that the Google / Apple API relies on Bluetooth over GPS; is fully opt-in; collects no personal or location data; only contacts a server if the user tests positive; and is primarily decentralized, relying on local storage of data, are all strong points to better ensure data privacy and security.

Yet, while many of these tools have been built with data privacy and security in mind, uptake has been slow and they have seen limited widespread adoption since their development in March and April 2020.[22] This might be due to the U.S.'s premature reopening with devastating health effects, as well as the many technical and ethical concerns the technologies raise, such as their questionable effectiveness, the ability for re-identification to still take place, as well as the likelihood of exacerbating existing disparities in pandemic impact. The myriad concerns raised by the use of these interventions—in concert with existing public health surveillance or on their own—are addressed below.

What concerns are raised?

1) Questionable effectiveness

Whether these interventions prove useful depends on two factors: 1) their use within a broader public health response, including the availability of widespread testing; and 2) the effectiveness of the technology itself.

Any use of location data or exposure notification to facilitate contact tracing will be in vain if not accompanied by widespread, accurate diagnostic

[21] Chan et al., "PACT," 13; Hart et al., "Outpacing the Virus," 16-17; Ashkan Soltani, Ryan Calo, and Carl Bergstrom, "Contact-tracing apps are not a solution to the COVID-19 crisis," Brookings, April 27, 2020, https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

[22] Hall, "Which States"; Chas Kissick, Elliot Setzer, and Jacob Schulz, "What Ever Happened to Digital Contact Tracing?" Lawfare, July 21, 2020, https://www.lawfareblog.com/what-ever-happened-digital-contact-tracing; Jonathan Zittrain, "Is Digital Contact Tracing Over Before It Began?" Medium, June 25, 2020, https://medium.com/berkman-klein-center/is-digital-contact-tracing-over-before-it-began -925c72036ee7.

and serological testing; a sufficient workforce of in-person tracers; the adequate provision of quarantine sites for those unable to self-isolate; and increased employer and healthcare protections, as well as social support for those who must quarantine or cannot go to work.[23] The U.S. currently lacks sufficient provision of all of these, with testing still far from the scale required to be effective and unevenly distributed across the country.[24] In late June, Dr. Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases, noted that contact tracing across the country was "not going well," while the shortage of personal protective equipment (PPE) remained an issue in July as cases flared, five months after shortages were originally identified.[25]

Against this grim backdrop, proximity apps, as experts at the Electronic Frontier Foundation (EFF) point out, might not be helpful in assisting contact tracing efforts with so many sheltering-in-place, the lack of sufficient testing, and the prevalence of asymptomatic cases.[26] The success and accuracy of these interventions also rely on a high-level of participation by the general public, necessitating use among up to 50-70% of the population according to some studies.[27] This requires trust in the entities collecting and storing data, a trust largely lacking across the U.S. according to recent studies.[28]

[23] This was noted in the majority of sources, panels, and interviews drawn on for this report. WHO's statement on this provides an excellent summary: "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing," World Health Organization, May 28, 2020, https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1; see also Margaret Bourdeaux, Mary L. Gray, and Barbara Grosz, "How human-centered tech can beat COVID-19 through contact tracing," The Hill, April 21, 2020, https://thehill.com/opinion/technology/493648-how-human-centered-technology-can-beat-covid-19-through-contact-tracing.

[24] Margaret Bourdeaux, Beth Cameron, and Jonathan Zittrain, "Testing Is on the Brink of Paralysis. That's Very Bad News," New York Times, July 16, 2020, https://www.nytimes.com/2020/07/16/opinion/coronavirus-testing-us.html?searchResultPosition=5; Katherine J. Wu, "Testing Backlogs May Cloud the True Spread of the Coronavirus," New York Times, July 19, 2020, https://www.nytimes.com/2020/07/19/health/coronavirus-testing-viral-spread.html?searchResultPosition=6.

[25] Quote in Feuer, "Contact Tracing"; Andrew Jacobs, "Grave Shortages of Protective Gear Flare Again as Covid Cases Surge," New York Times, July 8, 2020, https://www.nytimes.com/2020/07/08/health/coronavirus-masks-ppe-doc.html; William Wan, "America is running short on masks, gowns and gloves. Again," Washington Post, July 8, 2020, https://www.washingtonpost.com/health/2020/07/08/ppe-shortage-masks-gloves-gowns/.

[26] Andrew Crocker, Kurt Opsahl, and Bennett Cyphers, "The Challenge of Proximity Apps For COVID-19 Contact Tracing," Electronic Frontier Foundation, April 10, 2020, https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing.

[27] Hart et al., "Outpacing the Virus," 15; Oxford, "Digital contact tracing."

[28] Brooke Auxier, "How Americans see digital privacy issues amid the COVID-19 outbreak,"

Such trust is especially low among communities of color, as a result of a long history of targeted surveillance, medical experimentation, and racial bias in access to adequate healthcare and treatment.[29] In addition, exposure notification tools could ultimately prove ineffective to public health entities due to the limited data that they share with those authorities; while this is crucial for preserving privacy, it could limit the larger public health response by offering only a partial view of the information needed to assist contact-tracing efforts.[30]

Beyond the need for these interventions to assist a larger public health response, there are also concerns about whether the technology itself is fit for purpose. Location data—whether collected via Bluetooth, cell phones, or GPS—are not accurate enough to detect close contact with enough reliability to be effective, writes the ACLU.[31] The ability for proximity technology to accurately assess whether a user has been "too close for too long"—within six feet for over 15 minutes—is perhaps one of the greatest challenges the technology faces.[32] In the case of BLE technology specifically, detection could prove faulty, as sensing struggles to differentiate between actual contact and "contact" with your neighbor separated by a wall, floor, or between strangers in different subway cars. This could disproportionately

Pew Research Center, May 4, 2020, https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/?mkt_tok=eyJpIjoiTlRFNE1tWmxZMlEyWkRSbSIsInQiOiJkbGtwTjhUTDN5MngzbkpCT0xsd0hUWGp2QzVOTndYTFRleWtlQTR3OHRRVUdGa2tPUGwyTUpwbzAzeEFrQkZcL2JYd09xZlZmUGZjSDJkWUtkRHFsRGszRW9KWERlNFwvUkN2b2Fxc3UxM2VtS3pMNTUwbU0wUnM5ZkFoT1FlR3VZIn0=; Margaret Talev, "Axios-Ipsos Coronavirus Index Week 9: Americans hate contact tracing," Axios-Ipsos, May 12, 2020, https://www.axios.com/axios-ipsos-coronavirus-week-9-contact-%20tracing-bd747eaa-8fa1-4822-89bc-4e214c44a44d.html.

[29] Kade Crockford, "The Trump administration's war on immigrants, public trust, and tech-assisted contact tracing," Medium, June 25, 2020, https://medium.com/berkman-klein-center/the-trump-administrations-war-on-immigrants-public-trust-and-tech-assisted-contact-tracing-cede72687447; Katelyn Esmonde, "For contact tracing to work, public health authorities must regain the trust of Black communities," Vox, June 23, 2020, https://www.vox.com/first-person/2020/6/23/21299241/contact-tracing-covid-distrust-black-americans; Marya T. Mtshali, "How medical bias against black people is shaping Covid-19 treatment and care," Vox, June 2, 2020, https://www.vox.com/2020/6/2/21277987/coronavirus-in-black-people-covid-19-testing-treatment-medical-racism.

[30] Reed Albergotti and Drew Harwell, "Apple and Google are building a virus-tracking system. Health officials say it will be practically useless," Washington Post, May 15, 2020, https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/.

[31] Jay Stanley and Jennifer Stisa Granick, "The Limits of Location Tracking in an Epidemic," ACLU, April 8, 2020, https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic.

[32] Ron Rivest, "Privacy-preserving contact-tracing projects: PACT," July 28, 2020, Online panel presentation at the Responsible Data Summit, July 28-30, 2020.

affect those who live in densely populated neighborhoods and apartment buildings, individuals who are already disproportionately affected by the virus itself.[33] BLE also does not distinguish between types of interactions—whether in passing, prolonged contact, or if personal protective equipment was being used—and, therefore, the degree of risk posed by the interaction.[34] These factors increase the potential for over-notification of exposure, causing unnecessary anxiety and burden on users, as well as eroding trust in the system.[35] Over-notification could also result in overwhelming the health system further, both with the sheer amount of data collected by these apps and by an increased demand for testing fueled by unnecessary notifications.[36] In addition, technical concerns about Bluetooth's effect on battery drainage, as well as how well it works when running in the background (if multiple apps are open, say) are also potential barriers to the effectiveness of such an intervention.[37]

The opposite phenomenon could occur as well: instead of over-exposure, these apps could miss many potentially contagious encounters. Not everyone has a smartphone, of course,[38] and, if they do, they might not be carrying it with them all the time. Given the difficulty and uneven access to testing throughout the U.S., as well as the potential for false negatives, the verification of positive test results could prove difficult. These apps, of course, also do not account for false negatives nor asymptomatic positive cases without testing. Such a partial view of exposure could result in some users gaining a false sense of security.[39]

While undoubtedly the most privacy-preserving approach, the lack of evidence that BLE technology can accurately detect proximity to those who have tested positive, the potential for error, and the consequent negative effects for an already-strained healthcare system should be cause for

[33] Soltani et al., "Contact-tracing apps."

[34] Crocker, Opsahl, and Ciphers, "Challenge of Proximity Apps."

[35] Soltani et al., "Contact-tracing apps"; Raskar et al., "Apps Gone Rogue"; Sidney Fussell and Will Knight, "The Apple-Google Contact Tracing Plan Won't Stop Covid Alone," Wired Magazine, April 14, 2020, https://www.wired.com/story/apple-google-contact-tracing-wont-stop-covid-alone/.

[36] "Creating the Coronopticon," The Economist, March 26, 2020, https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic; Fussel and Knight, "Contact Tracing Plan."

[37] Rivest, "PACT."

[38] "Mobile Fact Sheet" Pew Research Center, June 12, 2019, https://www.pewresearch.org/internet/fact-sheet/mobile/.

[39] Raskar et al., "Apps Gone Rogue."

concern. Such approaches are ill-advised unless they prove to be fit for purpose in facilitating manual contract-tracing efforts based on current public health needs.

2) Data could be re-identified

Beyond these technical challenges, the risk remains that user data could be compromised. As many have noted, privacy in the context of COVID-19 is not an all-or-nothing choice, but a set of difficult trade-offs between utility, efficacy, and privacy, where "privacy-preserving" can come to take on different meanings.[40]

In the case of proximity tracing applications, the potential for health, location, and association information to be either re-identified or accessed by an unwanted third party is still present. While centralized data storage risks large-scale data breach, decentralized device storage could open additional opportunities to re-identify data, even if personal information is not collected on the applications.[41] Such identification can occur through inference or observation. If a user has only been in contact with one other person in the 24-hour period in which they received the notification, for example, it is likely they know who that person is.[42] Identification could also occur through more subversive means. Replay attacks, for example, where an adversary hacks into and replicates a previously authorized report to purposefully multiply exposure notifications are still possible in a decentralized system.[43] A user's health status could be revealed by what are called "correlation attacks," or a user's movements (by observation or by camera) being correlated with the information provided to the app.[44] Alternatively, if an app server collects the IP address of a device uploading

[40] Jennifer Daskal et al., "Privacy in the Age of COVID-19: Public Health and Individual Rights," Online panel presentation at the Internet Government Forum-USA, July 23, 2020, https://www.igfusa.us/privacy-in-the-age-of-covid-19-public-health-and-individual-rights/.

[41] Julia Angwin, "Will Google's and Apple's COVID Tracking Plan Protect Privacy?" The Markup, April 14, 2020, https://themarkup.org/ask-the-markup/2020/04/14/will-googles-and-apples-covid-tracking-plan-protect-privacy; Albert Fox Cahn and Evan Selinger, "Tracking coronavirus with smartphones isn't just a tech problem," Boston Globe, April 17, 2020, https://www.bostonglobe.com/2020/04/17/opinion/tracking-coronavirus-with-smartphones-isnt-just-tech-problem/; Serge Vaudenay, "Analysis of DP3T Between Scylla and Charybdis," April 8, 2020, https://eprint.iacr.org/2020/399.pdf.

[42] Soltani et al., "Contact-tracing apps."

[43] Chan et al., "PACT," 6; Vaudenay, "Analysis of D3PT," 6-7.

[44] Andy Greenberg, "Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered," Wired Magazine, April 17, 2020, https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses/; Soltani et al., "Contact-tracing apps."

Bluetooth beacon keys, even if the data itself are anonymized, this would allow for possible re-identification of the user if the app did not bar the collection of this information.[45] Stolen or seized phones, of course, could also put the data held in the device at risk.[46]

Other apps downloaded to the device could scrape or listen in to proximity-tracing data and send it to a third party.[47] Such third-party apps could have inadvertent access to the data, despite a published privacy policy, as demonstrated by North Dakota and South Dakota's Care19 app where Foursquare was inadvertently sent user data.[48] These proximity apps could also be hacked or trolled, with the risk of hackers fabricating positive reports to suppress voting or close schools in a particular district.[49] Bluetooth beacons are already used for ad-tracking and commercial purposes, collected by third parties for "proximity marketing."[50] Abuse of these applications for such purposes would require Google and Apple, as well as other app developers, to continue blocking advertiser access to this information. Additionally, the technology could be reappropriated by governments, who could exploit associational information for the purposes of immigration and law enforcement.[51] As such, all of these applications should strictly limit the amount of data collected, as well as conditions under which it is shared, accessed, and retained. Standard data security and encryption methods should be used, and such apps should bar usage for commercial purposes or by law enforcement (see section on additional requirements below).

[45] Greenberg, "Privacy Risk?"

[46] Chan et al., "PACT," 6.

[47] Angwin, "Tracking Plan"; Hart et al., "Outpacing the Virus," 25.

[48] Geoffrey A. Fowler, "One of the first contact-tracing apps violates its own privacy policy," Washington Post, May 21, 2020, https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/; Tim Starks, "Early Covid-19 tracking apps easy prey for hackers, and it might get worse before it gets better," Politico, July 6, 2020, https://www.politico.com/news/2020/07/06/coronavirus-tracking-app-hacking-348601. This issue has reportedly been fixed, however: "Care19 Update: Foursquare allows developers to disable IDFA collection," Jumbo Privacy, June 5, 2020, https://blog.jumboprivacy.com/care19-update-foursquare-allows-developers-to-disable-idfa-collection.htm.

[49] Angwin, "Tracking Plan"; Soltani et al., "Contact-tracing apps."

[50] Angwin, "Tracking Plan."

[51] Cahn and Selinger, "Tracking coronavirus"; Byron Tau and Michelle Hackman, "Federal Agencies Use Cellphone Location Data for Immigration Enforcement," Wall Street Journal, February 7, 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?mod=hp_lead_pos5.

3) Could exacerbate existing inequalities

In addition to their questionable efficacy and the privacy concerns they raise, the use of proximity-tracing applications has the potential to exacerbate existing inequities already laid bare by the pandemic. Black, Latinx, and Indigenous communities in this country are contracting and dying of COVID-19 at disproportionate rates, a result of centuries of systemic racism and settler colonial ideals that continue to structure access to healthcare, housing, employment, and clean water, as well as the current provision of adequate testing and treatment during the pandemic itself.[52] The use of these tools could also intensify the already disproportionate vulnerability of communities of color to hacking and data overreach.[53] Additionally, as Nicole Triplett, Director of Policy for Data for Black Lives points out, the use of these apps by the general public could result in the increased use of law enforcement against Black and Latinx communities, compounding the already disproportionate arrest rate of Black people in response to social distancing enforcement.[54]

As such applications require smartphones and access to the internet or a data plan, they cannot be used by, nor are designed for, those without access to such technology or by households who share phones. Smartphone use varies by race and ethnicity, age, income, as well as location in rural or urban areas, which could prove to exacerbate existing digital divides that

[52] Maria Godoy and Daniel Wood, "What Do Coronavirus Racial Disparities Look Like State By State?" NPR, May 30, 2020, https://www.npr.org/sections/health-shots/2020/05/30/865413079/what-do-coronavirus-racial-disparities-look-like-state-by-state; Rebecca Nagle, “Native Americans being left out of US coronavirus data and labelled as ‘other,’” The Guardian, April 24, 2020, https://www.theguardian.com/us-news/2020/apr/24/us-native-americans-left-out-coronavirus-data; Hollie Silverman et al., “Navajo Nation surpasses New York state for the highest Covid-19 infection rate in the US,” CNN Online, May 18, 2020, https://edition.cnn.com/2020/05/18/us/navajo-nation-infection-rate-trnd/index.html; Keeanga-Yamahtta Taylor, "The Black Plague," New Yorker, April 16, 2020, https://www.newyorker.com/news/our-columnists/the-black-plague; Jamelle Watson-Daniels et al., “Data for Black Lives COVID-19 Movement Pulsecheck and Roundtable Report,” Data for Black Lives, April 2020, d4bl.org/reports.html.

[53] "Mobile Location Data and Covid-19: Q&A,” Human Rights Watch, May 3, 2020, https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa#; Susan Landau, Christy E. Lopez, and Laura Moy, "The Importance of Equity in Contact Tracing,” Lawfare, May 1, 2020, https://www.lawfareblog.com/importance-equity-contact-tracing.

[54] Nicole Triplett, “Coronavirus contact tracing apps aren't worth the health risk to Black and Latinx people,” Boston Globe, June 24, 2020, https://www.bostonglobe.com/2020/06/25/opinion/coronavirus-contact-tracing-apps-arent-worth-health-risk-black-latinx-people/; Ashley Southall, “Scrutiny of Social-Distance Policing as 35 of 40 Arrested Are Black,” New York Times, May 7, 2020, https://www.nytimes.com/2020/05/07/nyregion/nypd-social-distancing-race-coronavirus.html.

privilege white, well-educated, and wealthier Americans living in nonrural areas.[55] Access to these applications might also be more difficult for many non-English speakers, those with disabilities or visual impairments, as well as those with limited technical literacy including the elderly.[56] The Bluetooth technology these apps utilize might not be accurate enough to detect and notify users in densely populated neighborhoods or apartment buildings with precision, making it more likely to induce false positives in those locations.[57]

There is also the fear that the use of such tracking applications becomes mandatory by employers or for access to certain spaces. As privacy scholar Paul Schwartz points out, “the critical issue is how the government and private sector will restrict access to spaces and opportunities based on whether or not one ‘consents’ to the use of an app or other monitoring device.”[58] If such technology does become mandatory, those performing essential functions—more often women and specifically women of color[59]—could have greater representation in the app, forcing potentially unnecessary quarantine and subsequent anxiety, stigma, and loss of income due to a higher rate of false positives.[60] This privileges those who can more easily “opt-out” by working from home, a luxury less accessible to Black and Hispanic workers.[61]

Widespread use of proximity applications, even if they have the potential to protect personal information, portend the continued expansion of the country’s surveillance infrastructure now and post-pandemic, what Woodrow Hartzog of Northeastern University calls “surveillance inertia.”[62]

[55] Pew, “Mobile Fact Sheet”; Andrew Perrin, “Digital gap between rural and nonrural America persists,” Pew Research Center, May 31, 2019, https://www.pewresearch.org/fact-tank/2019/05/31/digital-gap-between-rural-and-nonrural-america-persists/.

[56] Landau, Lopez, and Moy, “Importance of Equity.” See this same source for a thorough explanation of the potential inequities intensified by digital contact tracing tools.

[57] Ibid., Soltani et al., “Contact-tracing apps.”

[58] Paul Schwartz,"Illusions of consent and COVID-19-tracking apps," IAPP, May 19, 2020, https://iapp.org/news/a/illusions-of-consent-and-covid-tracking-apps/.

[59] Campbell Robertson and Robert Gebeloff, “How Millions of Women Became the Most Essential Workers in America,” New York Times, April 18, 2020, https://www.nytimes.com/2020/04/18/us/coronavirus-women-essential-workers.html?smid=nytcore-ios-share.

[60] Landau, Lopez, and Moy, “Importance of Equity.”

[61] Elise Gould and Heidi Shierholz, "Not everybody can work from home,” Economic Policy Institute, March 19, 2020, https://www.epi.org/blog/black-and-hispanic-workers-are-much-less-likely-to-be-able-to-work-from-home/.

[62] Woodrow Hartzog, "Op-Ed: Coronavirus tracing apps are coming. Here’s how they could

Even if these applications are designed for public health purposes only, these changes in application and device infrastructure, APIs, and what we consider to be "normal" use and access to our data today could lay the groundwork for increased surveillance by governments, schools, and employers in the future. Governments, as the EFF points out, can ask the developer to change the scope or request permission to access the data at a later time for different purposes.[63] Just as the surveillance state was able to expand uninhibited after 9/11, with some of the most troubling provisions of the Patriot Act only expiring a few months ago, the same could take place post-pandemic.[64] Surveillance in the name of public health could easily mutate into surveillance of the population, a "watching over" with a history of actively targeting Black and immigrant communities.[65]

Even if increased surveillance by other actors is largely abated, the development of these apps for public health purposes allows these firms to amass "infrastructural power" that secures their already-existing dominance in the tech market. As Michael Veale of University College London writes, such power increases the ability for Google and Apple to influence decision-making, control data and visibility, and produce change for a huge percentage of the population.[66] Google and Apple "are exercising sovereign power. It's just crazy,' said Matt Stoller, the director of research at the American Economic Liberties Project, a Washington think tank devoted to reducing the power of monopolies. Apple and Google have 'decided for the whole world,' he added, 'that it's not a decision for the public to make.'"[67] In taking on such a sovereign quality, they oppose the state in

reshape surveillance as we know it," LA Times, May 12, 2020, https://www.latimes.com/opinion/story/2020-05-12/coronavirus-tracing-app-apple-google.

[63] Crocker et al., "Challenge of Proximity Apps."

[64] Hartzog, "Reshape Surveillance"; Adam Klein and Edward Felten, "The 9/11 Playbook for Protecting Privacy," Politico, April 4, 2020, http://tiny.cc/Iro0tz; Andrew Roth et al., "Growth in surveillance may be hard to scale back after pandemic, experts say," The Guardian, April 14, 2020, https://www.theguardian.com/world/2020/apr/14/growth-in-surveillance-may-be-hard-to-scale-back-after-coronavirus-pandemic-experts-say.

[65] Simone Browne, Dark Matters: On the Surveillance of Blackness (Durham and London: Duke University Press, 2015); Allissa Richardson, Mutale Nkonde, and Apryl Williams, "Surveilling Black Lives," Theorizing the Web, July 16, 2020, https://www.youtube.com/watch?v=mYaJQAhUEM4. See also "The Color of Surveillance" conference series hosted by Georgetown Law (2016-2019), https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2019/.

[66] Michael Veale, "Privacy is not the problem with the Apple-Google contact-tracing toolkit," The Guardian, July 1, 2020, https://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights?CMP=fb_a-technology_b-gdntech.

[67] Quoted in Albergotti and Harwell, "Virus-Tracking System."

a seemingly different trade-off: whether it is safer for health data to be held by a tech giant or the government, neither of which have clean track records when it comes to protecting privacy for the public good.

What requirements are needed to protect user privacy?

Given the likelihood that such applications could exacerbate the disparate health and financial impacts of the pandemic, technological experts should proceed with caution when considering the use of exposure notification tools. As discussed in a June panel featuring technology and public health experts, technological expertise might best be refocused on reducing existing bottlenecks in the larger contact tracing and healthcare infrastructure as identified and called for by public health authorities and frontline healthcare workers.[68] They note that energy could be better spent on improving technology designed to facilitate the sharing of protected information between contact tracing and case management teams, patient access to information and care, and facilitating social support for those forced to quarantine and miss work due to illness.[69]

If the focus remains on exposure notification and other location-based contact tracing tools, however, strict requirements must be in place. In the absence of comprehensive federal legislation governing data privacy in the U.S., identifying which regulations might govern these new technologies continues to evolve. The relevant regulations to protect against the concerns highlighted above depend on the jurisdiction in which the application falls, whose data are being collected, and which entity holds and/or distributes the data.[70] While some of the legislation governing the technologies listed in this report will be discussed in Part Three, privacy experts and human rights advocates have identified a number of requirements beyond regulation that would safeguard user civil liberties.

[68] Margaret Bourdeaux et al., "Contact tracing: what it is, how it works, how tech can help," Online panel hosted by COVID-19 Technology Task Force, June 17, 2020, https://techcrunch.com/2020/06/16/j oin-us-june-17-for-a-live-discussion-on-covid-19-contact-tracing-and-safe-reopening-strategies/

[69] Ibid.

[70] For a thorough review of legislation that applies to digital contact tracing technology, see Chapter 4, "Legal Considerations," in Jeffrey Kahn, ed., Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance (Baltimore: Johns Hopkins University Press, 2020): 75-94.

Use limitations:

- Interventions must be "legal, necessary, and proportionate" according to international human rights law, in order to ensure effectiveness while not infringing on privacy and civil liberties.[71]

- They should be limited to pandemic use only, driven by public health expertise based on evidence that they are fit for purpose.[72]

- App use should always be voluntary and opt-in, with the ability to edit or delete the information provided at any time. The user should also be able to turn off BLE and the device, and withhold information as they would in a manual contact tracing interview.[73]

- Use of these applications or the data they collect should never be a requirement for any government services, employment, access to specific locations, nor be used for any punitive purposes.[74]

Public consultation and guidance:

- Applications need to be designed in consultation with and center the most affected communities; developers should seek active and meaningful participation and feedback in order to build public trust.[75]

- Developers should establish feedback mechanisms to integrate public responses regarding the effectiveness of such applications, questions, or concerns with its use, and provide active follow up to all inquiries.

Integration of privacy-by-design principles:

- Apps should integrate data minimization, encryption, security protocols,

[71] "Responsible Data Use Playbook for Digital Contact Tracing," Brighthive and the Future of Privacy Forum, 2020, https://playbooks.brighthive.io/contact-tracing/; Human Rights Watch, "Q&A"; Elizabeth Renieris, "When Privacy Meets a Pandemic," Medium OneZero, March 23, 2020, https://onezero.medium.com/when-privacy- meets-pandemic-fbf9154f80b3.

[72] Brighthive and Future of Policy Forum, "Playbook"; Kahn, Digital Contact Tracing.

[73] Crocker et al., "Challenge of Proximity Apps."

[74] Ibid.; Gillmor, "Principles," 5; Human Rights Watch, "Q&A"; Watson-Daniels et al., "Movement Pulsecheck," 26; World Health Organization, "Ethical Considerations," 3.

[75] Brighthive and Future of Policy Forum, "Playbook"; Human Rights Watch, "Q&A"; Watson-Daniels et al., "Movement Pulsecheck," 22-4; World Health Organization, "Ethical Considerations," 5.

and decentralized storage. The data, applications, and APIs should also commit to expiration once the pandemic is over.[76]

- Data collection should be transparent, with full disclosure of usage and data sharing.[77] This includes the use of open source code for all apps (already the case for many of these protocols such as D3-PT, Covid Watch, and CoEpi), which should be subject to third-party review.[78]

Oversight, testing, and evaluation:

- Applications should be tested before use and at every phase of the development process, using "commonly accepted practices such as security auditing, bug bounties, and abusability testing to identify vulnerabilities and unintended consequences of a potentially global new technology."[79]

- Impact assessments of application effectiveness and ethical considerations should be conducted and repeated in order to ensure the continued utility of the intervention.[80]

- Applications should actively mitigate differential inclusion and address potential bias, so as not to exacerbate existing inequalities or disproportionately affect already marginalized groups.[81]

- There should be independent oversight of both the public health agencies and the companies developing the technology with appropriate accountability and recourse mechanisms in place for users.[82]

[76] Brighthive and Future of Policy Forum, "Playbook"; Crocker et al., "Challenge of Proximity Apps"; Gillmor, "Principles," 8; Human Rights Watch, "Q&A"; Soltani et al., "Contact-tracing apps."

[77] Crocker et al., "Challenge of Proximity Apps"; Human Rights Watch, "Q&A."

[78] Gillmor, "Principles," 10-11.

[79] Soltani et al., "Contact-tracing apps." See also: Human Rights Watch, "Q&A"; World Health Organization, "Ethical Considerations," 3.

[80] Brighthive and Future of Policy Forum, "Playbook"; Daskal et al., "Privacy."

[81] Crocker et al., "Challenge of Proximity Apps"; Gillmor, "Principles," 6-7; Human Rights Watch, "Q&A."

[82] Brighthive and Future of Policy Forum, "Playbook"; Human Rights Watch, "Q&A"; Kahn, Digital Contact Tracing, 73-4; World Health Organization, "Ethical Considerations," 5.

AGGREGATED LOCATION DATA

Another category of technology being deployed throughout the pandemic is anonymized, aggregated location data, designed for use by researchers, epidemiologists, public health officials, and nonprofits to better understand the spread of the virus and the effectiveness of social distancing orders.

How does it work?

Aggregated location data is location information—often already collected in massive datasets by social media platforms, mobile ad and location companies—that is anonymized and bundled at specific geographic scales in order to prevent individual identification.[83] As discussed in the previous section of this report, de-identified or anonymized data always have the potential to be re-identified,[84] often in surprisingly invasive ways. As the *New York Times* reported in 2018 and 2019, anonymized location data scraped from apps downloaded to a user's phone can be re-identified by inference to an incredible level of detail—logging when a user's device goes to the office, health clinic, or their children's school—revealing potentially stigmatizing personal information.[85] Aggregation is the crucial privacy-preserving step, where bundling location information by county or state can make its re-identification more difficult.[86] Sometimes, as with Facebook and Google's respective approaches to differential privacy, artificial noise can also be added to the dataset to further protect privacy while maintaining accuracy of the data.[87] While anonymized aggregation is less cause for concern, it should still

[83] For a more thorough description of aggregation, see: Jacob Hoffman-Andrews and Andrew Crocker, "How to Protect Privacy When Aggregating Location Data to Fight COVID-19," Electronic Frontier Foundation, April 6, 2020, https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19.

[84] For more on re-identification, see: Sara Harrison, "When is Anonymous Not Really Anonymous?" The Markup, March 24, 2020, https://themarkup.org/ask-the-markup/2020/03/24/when-is-anonymous-not-really-anonymous.

[85] Jennifer Valentino-DeVries et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," New York Times, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?smid=re-nytimes; Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," New York Times, December 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[86] Mana Azarmi and Andy Crawford, "Use of Aggregated Location Information and COVID-19: What We've Learned, Cautions about Data Use, and Guidance for Companies," Center for Democracy and Technology, 2020, 4, https://cdt.org/wp-content/uploads/2020/05/2020-05-29-Use-of-Aggregated-Location-Information-and-Covid-19.pdf

[87] Adam Sadilek and Xerxes Dotiwalla, "New Insights into Human Mobility with Privacy Preserving Aggregation," Google AI Blog, November 12, 2019, https://ai.googleblog.

be considered as a set of tradeoffs between privacy and value of the data collected, as the risk of identification always remains.[88]

Select examples of such aggregated data projects are Cuebiq's Mobility Insights, Camber Systems' Social Distancing Reporter, Google's COVID-19 Community Mobility Reports, Facebook's Population Density and Disease Prevention Maps, and Apple's Mobility Trends.[89] Once the data are aggregated, they are then released, visualized, and shared with the public, universities, non-profits, and the government for research purposes. Cuebiq's data were used in *New York Times* reporting on American adherence to shelter-in-place orders,[90] for example, while Facebook's mobility data has been used by the State of California to assess the effectiveness of social distancing measures.[91] In many cases, these tech giants and smaller firms that collect location information already had access to this data and are now attempting to mobilize it for social good.

Why use this intervention?

The primary justification for use of this data is the mobilization of an existing resource to generate new and needed epidemiological knowledge about a virus we still know little about. Such data are considered by epidemiologists, such as those affiliated with the COVID-19 Mobility Data Network, to be a crucial tool for analyzing trends in population mobility in order to assess the effectiveness of COVID-19 containment policies, such as shelter-in-place orders by location or

com/2019/11/new-insights-into-human-mobility-with.html.

[88] Hoffman-Andrews and Crocker, "Protect Privacy."

[89] "Mobility Insights," Cuebiq, 2020, https://www.cuebiq.com/visitation-insights-covid19/; "Social Distance Reporter," Camber Systems, 2020, https://covid19.cambersystems.com/about/; Jen Fitzpatrick and Karen DeSalvo, "Helping public health officials combat COVID-19," Google Health, April 3, 3030, https://www.blog.google/technology/health/covid-19-community-mobility-reports?hl=en; "COVID-19 Community Mobility Reports," Google, 2020, https://www.google.com/covid19/mobility/; "Our Work on COVID-19," Facebook Data for Good, 2020, https://dataforgood.fb.com/docs/covid19/; "Mobility Trends Reports," Apple, 2020, https://covid19.apple.com/mobility.

[90] Jennifer Valentino-DeVries, Denise Lu, and Gabriel J.X. Dance, "Location Data Says It All: Staying at Home During Coronavirus Is a Luxury," New York Times, April 3, 2020, https://www.nytimes.com/interactive/2020/04/03/us/coronavirus-stay-home-rich-poor.html; James Glanz et al., "Where America Didn't Stay Home Even as the Virus Spread," New York Times, April 2, 2020, https://www.nytimes.com/interactive/2020/04/02/us/coronavirus-social-distancing.html.

[91] Issie Lapowsky, "Facebook data can help measure social distancing in California," Protocol, March 17, 2020, https://www.protocol.com/facebook-data-help-california-coronavirus; Andrew Schroeder, "Mobility Data Essential to Stopping Covid-19, Reopening Cities and Counties," Direct Relief, April 20, 2020, https://www.directrelief.org/2020/04/mobility-data-essential-to-stopping-covid-19-re-opening-cities-and-counties/.

movement patterns as people start returning to work.[92] In addition, aggregated data are one of the least concerning uses of data when it comes to privacy and consumer protection, due to the pairing of anonymization and aggregation, which provides greater incentive for its use.

What concerns are raised?

The first concern such aggregated data raise is lack of disclosure or consent to use of the data for these new purposes. Much of this mobility data is simply a repackaging of location data that companies already possess for commercial purposes. Google, Apple, and Facebook have all posted disclosure notices of use policies on their websites, with opportunities to disable location data collection in some cases.[93] As EFF points out, however, data collected by data brokers through ads, cell phone providers, or private location companies might not meet consent and disclosure standards. Users are likely not actively consenting to this particular use of their data, which ideally should take place each time their data are used for a new purpose, even if consent was given before. Given the urgency of pandemic, EFF notes, it is unlikely that new consenting occurred for this aggregate use, therefore users should have the option to edit or delete their data at any time.[94] This still places the onus on the user, rather than the company collecting the data, to opt-out if they so choose.

A second concern is how representational the data are and the potential impact on future policy and public health decisions. Medical professionals and epidemiologists advocating for the use of aggregated location data at Harvard (also affiliated with the COVID-19 Mobility Data Network) have warned that not all COVID-19 data “can be trusted,” and therefore care must be taken to put the data into context, articulate its limits, and analyze accordingly.[95] Yet the means by which such data are collected—through smartphones or computers—limits the sample to those with access to such technologies, the internet, and necessary data plans. As a result, the data only represents a subsection of the population without sufficient sampling of those who may lack access, such as

[92] Caroline O. Buckee et al., “Aggregated mobility data could help fight COVID-19,” Science 368, no. 6487 (April 10, 2020): 145-146, https://doi.org/10.1126/science.abb8021; “COVID-19 Mobility Data Network,” COVID-19 Mobility Data Network, 2020, https://www.covid19mobility.org/.

[93] Azarmi and Crawford, “Location Information,” 5; Google, “Mobility Reports.”

[94] Hoffman-Andrews and Crocker, "Protect Privacy.”

[95] Satchit Balsari, Caroline Buckee, and Tarun Khanna, “Which Covid-19 Data Can You Trust?” Harvard Business Review, May 8, 2020, https://hbr.org/2020/05/which-covid-19-data-can-you-trust.

the elderly, those with lower income, or residents in rural areas.[96]

This method also has the potential to indicate certainty while simultaneously obscuring the more complex realities of movement hidden in the data. Higher rates of mobility in a neighborhood could indicate a greater proportion of essential workers still needing to commute or individuals looking for services or shelter, rather than a “breach” of social distancing requirements.[97] This could misdirect policy, resources, or the use of law enforcement, causing unnecessary harm to communities already more heavily affected by the virus, and poses the risk of flawed assessments about how the disease is spreading and how best to contain it.[98]

Government access to the data is also concerning, given the ease with which it could be re-identified and mobilized by law enforcement if not properly secured. In March, the U.S. government was in communication with Facebook and Google about the use of location data for pandemic response.[99] Just months prior, the government was reportedly purchasing and using aggregated data from location data firms for immigration and border enforcement.[100] It is not a far stretch to imagine that such data, collected in the name of a public health emergency, could be utilized for similar purposes. This paradox is also laid bare by the July announcement that federal data collection will bypass the CDC and now be controlled by the Department of Health and Human Services (HHS).[101] The new HHS data collection infrastructure, while managed by a

[96] Azarmi and Crawford, “Location Information,” 8-9; Hoffman-Andrews and Crocker, "Protect Privacy”; Amos Toh, “Big Data Could Undermine the Covid-19 Response,” Wired Magazine, April 12, 2020, https://www.wired.com/story/big-data-could-undermine-the-covid-19-response/.

[97] Hoffman-Andrews and Crocker, "Protect Privacy”; Toh, “Big Data.”

[98] Ibid.; Azarmi and Crawford, “Location Information,” 8-9.

[99] Tony Romm, Elizabeth Dwoskin, and Craig Timberg, "U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus," Washington Post, March 17, 2020, https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/; Byron Tau, "Government Tracking How People Move Around in Coronavirus Pandemic,” Wall Street Journal, March 28, 2020, https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202.

[100] Byron Tau and Michelle Hackman, "Federal Agencies Use Cellphone Location Data for Immigration Enforcement. The Wall Street Journal,” Wall Street Journal, February 7, 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?mod=hp_lead_pos5; The Editorial Board, “The Government Uses ‘Near Perfect Surveillance’ Data on Americans,” New York Times, February 7, 2020, https://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html.

[101] Sheryl Gay Stolberg, “Trump Administration Strips C.D.C. of Control of Coronavirus Data,” New York Times, July 14, 2020, https://www.nytimes.com/2020/07/14/us/politics/trump-cdc-coronavirus.html? campaign_id=9&emc=edit_nn_20200715&instance_id=20323&nl=the-morning&regi_id=71530125&segment_id=33439&te=1&user_

company called TeleTracking,[102] reportedly uses Palantir's Foundry and Gotham platforms, formerly used by ICE to facilitate the deportation and separation of undocumented families.[103] As Amnesty International poignantly asked in a *Washington Post* op-ed, "Why are we trusting a company with ties to ICE and intelligence agencies to collect our health information?"[104]

What requirements are needed to protect user privacy?

While aggregation mitigates a number of privacy concerns and can be leveraged for epidemiological research, such data should still include clear requirements for use, user consent, transparency, and external review:

- **Use and purpose limitations:** Location data should be aggregated to the highest level of generality, access should be limited to specific, vetted parties for specific pandemic-related purposes, should include sunset clauses and deletion requirements, in addition to commitments to not re-identify the data.[105]

- **Affirmative consent:** User consent should be secured at every stage of the process, with informed disclosure of how formerly-collected data might be repurposed for this new analysis, and with the opportunity to opt-out or delete collected data at any time.[106]

id=f4e7f5fa33790ffaee0ae774229c03c3.

[102] For concerns raised by the TeleTracking bid and contract itself, see Tim Mak and Dina Temple-Raston, "How Small Tech Company Got $10.2 Million Contract To Build COVID-19 Database," NPR, July 29, 2020, https://www.npr.org/2020/07/29/896840037/how-small-tech-company-got-10-2-million-contract-to-build-covid-19-database.

[103] Erin Banco and Spencer Ackerman, "Team Trump Turns to Peter Thiel's Palantir to Track Virus," The Daily Beast, April 21, 2020, https://www.thedailybeast.com/trump-administration-turns-to-peter-thiels-palantir-to-track-coronavirus?ref=scroll; Edward Ongweso Jr., "Palantir's CEO Finally Admits to Helping ICE Deport Undocumented Immigrants," Vice News, January 24, 2020, https://www.vice.com/en_us/article/pkeg99/palantirs-ceo-finally-admits-to-helping-ice-deport-undocumented-immigrants; Sara Morrison, "Everything you need to know about Palantir, the secretive company coming for all your data," Vox Recode, July 16, 2020, https://www.vox.com/recode/2020/7/16/21323458/palantir-ipo-hhs-protect-peter-thiel-cia-intelligence.

[104] Michael Kleinman and Charanya Krishnaswami, "Why are we trusting a company with ties to ICE and intelligence agencies to collect our health information?" Washington Post, May 21, 2020, https://www.washingtonpost.com/opinions/2020/05/21/why-are-we-trusting-company-with-ties-ice-intelligence-agencies-collect-our-health-information/.

[105] Azarmi and Crawford, "Location Information," 10; Hoffman-Andrews and Crocker, "Protect Privacy"; Toh, "Big Data."

[106] Ibid.

- **Transparency:** There should be full transparency in the aggregation methodology with appropriate context, the limits associated with such data including who is not represented, as well as how conclusions are being drawn to inform public health measures and potential risks associated.[107]

- **External review:** Experts should thoroughly review the methods and privacy safeguards in place for each dataset, as well as vetting the partners requesting the data to ensure user information is adequately protected and used in line with the conditions above.[108]

SYMPTOM-TRACKING APPLICATIONS

The development of symptom-tracking applications presents a different approach to data-driven pandemic response. Rather than rely on mobility data, these apps collect both individual and aggregated, longitudinal, self-reported data on risk factors and symptoms for COVID-19 directly from app users themselves in order to facilitate epidemiological and clinical research related to virus infection, treatment, and clinical outcomes. Given the speed at which the virus has spread, the wide range of symptoms and risk factors, and a lack of widespread testing, epidemiologists are proposing the use of mobile data collection in order to collect information in real-time at a large scale. As the COVID Symptom Study team writes, "Addressing this priority will allow for more accurate estimates of disease incidence, inform risk mitigation strategies, facilitate allocation of scarce testing resources, and encourage appropriate quarantine and treatment of those afflicted."[109] The apps could also serve a predictive capacity, with the ability for researchers to identify COVID-19 hotspots based on reported symptoms prior to positive test results. This data, the researchers hope, could then inform the prepositioning of supplies such as personal protective equipment, allocation of tests, relaxation of social distancing requirements, and could evaluate the success of public health interventions.

The most widely used application of this kind is the COVID Symptom Study (formerly known as the COVID Symptom Tracker) across the U.S. and the

[107] Azarmi and Crawford, "Location Information," 10; Balsari, Buckee, and Khanna, "Covid-19 Data"; Toh, "Big Data."

[108] Balsari, Buckee, and Khanna, "Covid-19 Data."

[109] David A. Drew et al., "Rapid implementation of mobile technology for real-time epidemiology of COVID-19," Science 368, no. 6497 (June 19, 2020): 1362-1367, https://doi.org/10.1126/science.abc0473.

U.K., with over four million users worldwide at the time of writing.[110] This app was designed by King's College London, Massachusetts General Hospital, and ZOE Global Limited, in partnership with the Harvard T.H. Chan School of Public Health and Stanford's School of Medicine. Other examples of similar applications include COVID Near You, a retrofitted version of the Flu Near You app, led by Boston Children's Hospital and Harvard Medical School; HowWeFeel, designed by Pinterest, Harvard, and MIT; and Apple's COVID-19 Screening Tool, sponsored by the White House, FEMA, and the CDC.[111]

How does it work?

These interventions are designed for use by the general public, over the age of 18, who download one of these symptom apps to their smartphones. In the case of the COVID Symptom Study, individuals can consent to their data being shared with existing clinical studies to facilitate data collection (consent that can be withdrawn and data deleted at any time). This app also targets healthcare workers to participate in data collection for study purposes.[112] Once a user downloads the app, they fill out a baseline questionnaire with demographic and health information, including age, sex, ZIP code, and symptom data. Some apps also collect additional demographic and health information including pre-existing risk factors.[113] Then, once a day, each user fills out a brief symptom survey—whether experiencing symptoms or not—to report how they feel. The data collected are then aggregated, anonymized, and often mapped publicly, and are sent to researchers and epidemiologists for analysis. The apps, primarily designed in partnership with epidemiologists at leading public health institutions, are intended for research conducted by those institutional partners. Data access can be requested, but—as in HowWeFeel's case—organizations are screened and must agree to a data access policy.[114] The data Apple collects through its COVID-19 Screening Tool is anonymized, aggregated, and sent to the CDC; it is reportedly not linked to any identifying data that Apple holds for its users.[115]

[110] "COVID Symptom Study," ZOE Global Limited, 2020, https://covid.joinzoe.com/us-2.

[111] "About Us," COVID Near You, 2020, https://covidnearyou.org/us/en-US/; "About" and "FAQ," HowWeFeel, 2020, https://howwefeel.org/; "COVID-19 Screening Tool," Apple, 2020, https://covid19.apple.com/screening.

[112] Drew et al., "Rapid implementation."

[113] "COronavirus Pandemic Epidemiology (COPE) Consortium," Mongan Institute, 2020, https://www.monganinstitute.org/cope-consortium.

[114] "Data Access Terms," HowWeFeel, 2020, https://howwefeel.org/data-access-terms/.

[115] Darrell Etherington, "Apple adds anonymous symptom and health info sharing to its

Why use this intervention?

The primary argument in favor of using these applications is that they are an easy and efficient way to collect data on risk factors and symptoms for COVID-19 at scale, in order to facilitate research on virus infection, treatment, and clinical outcomes. The most widely used application, the COVID Symptom Study, allowed scientists to confirm anosmia (the loss of taste and smell) as a leading symptom of COVID-19.[116] Designed as a technological tool for a very large-scale clinical research study, the app utilizes similar data protocols and protections and, as such, complies with the European Union's General Data Protection Regulation (GDPR), the U.S.'s Health Insurance Portability and Accountability Act (HIPAA), and is reviewed by individual Institutional Review Boards.[117] Other symptom-tracking apps are not subject to the same protocols, however, as the HIPAA Privacy Rules only apply to "covered entities" such as hospitals and health plan providers and their "business associates"[118]; unless an app is collecting information on behalf of one of these entities, no such rules apply.

While symptom-tracking apps collect a fair amount of personal information, in contrast to the aggregated location data discussed above, data submission is fully consented to and self-reported by the user. Data are anonymized and aggregated before being sent to other researchers, and are not used for commercial purposes. IP addresses are collected and recorded by some applications, such as COVID Near You, but remain confidential.[119] COVID Near You also promises not to "sell, share, rent, or otherwise reveal this information to any third party except as required by law," but might share the aggregated data with third parties in a way that's

COVID-19 app and website," TechCrunch, June 9, 2020, https://techcrunch.com/2020/06/09/apple-adds-anonymous-symptom-and-health-info-sharing-to-its-covid-19-app-and-website/.

[116] Umair Irfan, "Why it can be so hard to tell if you have Covid-19," Vox, May 11, 2020, https://www.vox.com/2020/4/2/21200217/coronavirus-symptoms-covid-19-fever-cough-smell-taste; Andrew Jacobs, "App Shows Promise in Tracking New Coronavirus Cases, Study Finds," New York Times, May 11, 2020, https://www.nytimes.com/2020/05/11/health/coronavirus-symptoms-app.html; Cristina Menni et al., "Real-time tracking of self-reported symptoms to predict potential COVID-19," Nature Medicine 26 (May 11, 2020): 1037-1040, https://doi.org/10.1038/s41591-020-0916-2.

[117] Mongan Institute, "COPE Consortium."

[118] "Who must comply with HIPAA privacy standards?" U.S. Department of Health and Human Services, 2002, https://www.hhs.gov/hipaa/for-professionals/faq/190/who-must-comply-with-hipaa-privacy-standards/index.html.

[119] "Privacy Policy," COVID Near You, 2020, https://covidnearyou.org/us/en-US/privacy.

kept anonymous.[120] The same conditions apply to the Symptom Study, which discloses the list of third party access in their Privacy Policy.[121]

What concerns are raised?

The concerns raised by symptom-tracking applications mirror those discussed in relation to aggregated location data above, particularly the representationality of the data and the ever-present risk of re-identification and unauthorized data sharing. In terms of representation, the self-reporting of symptoms does not necessarily align with a positive COVID-19 result (and is difficult to confirm given the lack of widespread and accurate testing), nor does the data collected by these apps capture asymptomatic positive cases within the data. There is also the chance that users could be reporting symptoms of other diseases.[122] The triaging of tests by the U.S. government (i.e., sending tests to certain locations, or prioritizing certain wealthy individuals within the testing pool due to limited resources) could inadvertently skew the results of the data as well.[123] Symptom data collection—as with all of the technological interventions discussed so far—is also limited to those using smartphones, and therefore lacks representation from groups who lack access or have limited access to such devices.

While app use is fully consent-based with symptoms self-reported, users still risk that the data could be re-identified and used by federal, state, and local governments for law enforcement purposes if privacy policies are breached. Data for these studies are also retained for an extended period of time, as this research is designed to inform responses to future pandemics as well. As such, full disclosure of risks, data usage, sharing, and retention is of utmost importance.

What requirements are needed to protect user privacy?

The majority of these apps include thorough disclosures for the use and sharing of data, restrict the use or selling of data for commercial purposes, and include data access agreements for requesting partners. There should also be full transparency as to how the data are being analyzed and

[120] Ibid.

[121] "COVID-19 Symptom Tracker App Privacy Policy US," Zoe Global Limited, March 27, 2020, https://storage.googleapis.com/covid-symptom-tracker-public/privacy-policy-us.pdf.

[122] Jacobs, "App Shows Promise."

[123] Kaiser Fung, "Beware the Lofty Promises of Covid-19 'Tracker' Apps," Wired Magazine, May 13, 2020, https://www.wired.com/story/beware-the-lofty-promises-of-covid-19-tracker-apps/.

limitations of the data (including representationality of the dataset and methodology), given the intention to inform both individual behavior and public health interventions. Clear instructions should be provided to users for how to opt-out or delete their data at any time. Partners who request the data should be adequately reviewed and screened to ensure that they will comply with data protection policies and have established appropriate safeguards.

It is imperative that standard privacy-preserving principles be utilized at every stage of the research process. As one of the leading researchers of the COVID Symptom Study told the *New York Times*, the collection of this data is “a sort of real-time experiment done on a massive scale that couldn’t have been done a couple of years ago.”[124] While such an experiment could yield incredibly useful epidemiological data, its unprecedented scale calls for increased attention to privacy and security.

IMMUNITY PASSPORTS

“Unless convincing evidence is presented, we should remain highly skeptical that immunity passports could be designed in such a way that leads to fair social outcomes rather than unjust discrimination and stigmatization that exacerbates inequality.”
- Mark Latonero, Technology and Human Rights Fellow, Carr Center for Human Rights Policy[125]

How does it work?

Immunity passports, or immunity-based licenses or certification, have been proposed in the U.S. and many countries around the world as a future intervention to facilitate individual movement as the country begins to reopen.[126] This “passport,” either in digital or paper form, would serve as documentary evidence that an individual has immunity to COVID-19 and could become a requirement for entry into certain spaces, participation

[124] Quote by Dr. Tim Spector, King’s College London, in Jacobs, “App Shows Promise.”

[125] Mark Latonero, Elizabeth Renieris, and Mathias Risse, "Examining the Ethics of Immunity Certificates,” Harvard Kennedy School, Carr Center Covid-19 Discussion Series, June 1, 2020, https://carrcenter.hks.harvard.edu/files/cchr/files/005-covid_discussion_paper.pdf.

[126] Adrianna Rodriguez, “Dr. Fauci says immunity certificates 'possible' after coronavirus pandemic. Here's what that means,” USA Today, April 16, 2020, https://www.usatoday.com/story/news/health/2020/04/16/covid-19-fauci-says-immunity-certificates-possible-what-they/2987765001/.

in certain activities, or for domestic and international travel as deemed appropriate by public health officials.

Why use this intervention?

Immunity passports are considered a means by which to ensure individual safety while opening up the economy and facilitate the movement of the general public, including international travel. It could give peace of mind to essential workers who are continuously exposed to the virus at work, for example, or potentially mitigate spread of the virus within certain high-risk settings such as hospitals and nursing homes.[127] There is precedent for such certification requirements, such as proof of immunization as a requirement for school attendance or the need to show a yellow fever vaccination card in order to enter certain countries. Yet, as Professors Mark Hall and David Studdert write in *JAMA*, “an immunity certificate program for COVID-19 would be unparalleled in several ways. First, because COVID-19 is not (yet) vaccine-preventable, inoculation must come entirely from prior infection. Second, the program likely would apply more broadly than to only a handful of selected professions or activities. Third, the conditioned ‘privileges’ could include a greater range of fundamental civil liberties and opportunities, like freedom of association, worship, work, education, and travel.”[128] The unprecedented nature of this intervention and the questions it leaves unanswered present significant risks. As such, immunity passports have garnered widespread condemnation and the consensus that such an intervention would do more harm than good.

What concerns are raised?

First, what constitutes “immunity” remains in question, especially with evidence of COVID-19 reinfection.[129] The WHO warns that it is unclear how

[127] Emily Mullin, "Immunity Passports’ Could Create a New Category of Privilege,” Medium OneZero, April 23, 2020, https://onezero.medium.com/immunity-passports-could-create-a-new-category-of-privilege-2f70ce1b905.

[128] Mark A. Hall and David M. Studdert, “Privileges and Immunity Certification During the Covid-19 Pandemic,” JAMA 323, no. 22 (May 6, 2020): 2243-2244, https://doi.org/10.1001/jama.2020.7712. For more on the differences COVID-19 presents, see: Alexandra L. Phelan, “COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges,” The Lancet 395, no. 10237 (May 4, 2020): 1595-1598, https://doi.org/10.1016/S0140-6736(20)31034-5; Elizabeth Renieris, Sherri Bucher, and Christian Smith, "The Dangers of Blockchain-Enabled ‘Immunity Passports’ for COVID-19,” Medium, May 18, 2020, https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290.

[129] Naman M. Aggarwal and Carolyn Tackett, “The impact of COVID-19 digital health certificates,” Access Now, July 2020, 4, https://www.accessnow.org/cms/assets/

much immunity antibodies create and for how long.[130] Declaring immunity based on false positives or with only a partial immunity rate could unintentionally continue the spread of the virus, exposing the "licensed" individual and others to potential infection.

Second, even if criteria for immunity are established, the production of such a certification would require widespread, accurate diagnostic and serological (antibody) testing country-wide, available to the entire population for free or at very low cost.[131] Testing would have to be performed twice, at minimum, to certify immunity, given the possibility that those tested could later become infected and have to be tested again. After the initial certification process, testing would have to continue on an annual basis for recertification.[132] The rapid rollout and increasing availability of unapproved antibody tests could induce individuals to self-certify and potentially ease self-restriction without thorough scientific consensus, providing a false sense of security and potentially driving more infections.[133]

Third, the requirement of immunity passports could create a two-tiered social structure, where immune individuals are allowed to work, move freely, and participate in society, while those without are confined to their homes for an undetermined period of time, often without sufficient financial support or adequate healthcare.[134] While some argue that

uploads/2020/07/Impact-COVID-19-digital-health-certificates.pdf; Hall and Studdert, "Immunity Certification"; Phelan, "Immunity Passports"; Renieris, Bucher, and Smith, "Dangers." On recent reinfection, see: Andrew Joseph, "Scientists are reporting several cases of Covid-19 reinfection — but the implications are complicated," STATNews, August 28, 2020, https://www.statnews.com/2020/08/28/covid-19-reinfection-implications/.

[130] "Scientific Brief: 'Immunity passports' in the context of COVID-19," World Health Organization, April 24, 2020, https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19.

[131] Esha Bhandari and ReNika Moore, "Coronavirus 'Immunity Passports' are not the Answer," ACLU, May 18, 2020, https://www.aclu.org/news/privacy-technology/coronavirus-immunity-passports-are-not-the-answer/.

[132] Natalie Kofler and Françoise Baylis, "Ten reasons why immunity passports are a bad idea," Nature 581 (May 21, 2020): 379-81, https://media.nature.com/original/magazine-assets/d41586-020-01451-0/d41586-020-01451-0.pdf.

[133] "Coronavirus (COVID-19) Update: FDA Issues Warning Letters to Companies Inappropriately Marketing Antibody Tests, Potentially Placing Public Health at Risk," U.S. Food and Drug Administration, June 17, 2020, https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-issues-warning-letters-companies-inappropriately-marketing-antibody; Hall and Studdert, "Immunity Certification"; Christina Morales, "F.B.I. Warns of Fraudulent Coronavirus Antibody Tests," New York Times, June 29, 2020, https://www.nytimes.com/2020/06/29/us/fake-coronavirus-antibody-test.html?searchResultPosition=2.

[134] Bhandari and Moore, "Immunity Passports"; Mullin, "Immunity Passports."

"accurate immunity certification could have a progressive valence that, conceivably, operates more as a leveler than class divider" given that potential immunity might be concentrated in groups disproportionately affected by the virus,[135] this is unlikely given the greater impact of the virus on Black, Latinx, and Indigenous communities caused by systemic inequities in access to healthcare, testing, and treatment. As the ACLU points out, "it is foreseeable, maybe even inevitable, that an immunity passport system, with all its attendant pressures on workers to acquire immunity, would result in disproportionately more illness and death among people of color in the U.S."[136] Those seeking immunity certification might be prevented from doing so with ease and at low cost, and the administration of certification itself could mirror existing inequities in access to testing, treatment, and care,[137] reifying the racialized, classed, and gendered impact of the pandemic through the use of such documentation.[138] Enforcement of immunity-based movement has the potential to do the same, impacting those already policed and profiled at greater rates.[139] Such certificates could also be used to suppress the exercise of other civil liberties, such as to "silence dissent, suppress social movements, or otherwise exert control for purposes other than public health."[140]

In addition, as Alexandra Phelan of Georgetown University's Center for Global Health Science and Security points out, until a COVID-19 vaccine is developed and widely available, immunity passports incentivize infection instead of vaccination.[141] There is widespread concern that, if such a passport is required without a vaccine available, individuals will expose or

[135] Hall and Studdert, "Immunity Certification."

[136] Bhandari and Moore, "Immunity Passports."

[137] Aggarwal and Tackett, "Digital Health Certificates," 8-10; Phelan, "Immunity Passports."

[138] The production of a racialized, two-tiered society via the possession of immunity has historical precedent. As historian Kathryn Olivarius's work demonstrates in great detail, immunity to yellow fever in antebellum New Orleans secured "immunocapital" for its white residents, while serving as justification for the continued enslavement of its Black population. "Black people could thus possess immunity, but not immunocapital, an expedient feint of logic that whites used to enrich themselves and reinforce their social and political dominance over blacks" (429) in Kathryn Olivarius, "Immunity, Capital, and Power in Antebellum New Orleans," The American Historical Review 124, no. 2 (April 2019): 425-455, https://doi.org/10.1093/ahr/rhz176. Also see Olivarius's recent New York Times op-ed on the topic in relation to the proposition of immunity passports for COVID-19: Kathryn Olivarius, "The Dangerous History of Immunoprivilege," New York Times, April 12, 2020, https://www.nytimes.com/2020/04/12/opinion/coronavirus-immunity-passports.html?smid=tw-share.

[139] Kofler and Baylis, "Ten Reasons"; Latonero, Renieris, and Risse, "Examining the Ethics."

[140] Aggarwal and Tackett, "Digital Health Certificates," 8.

[141] Phelan, "Immunity Passports."

infect themselves with the virus in order to secure immunity and return to work.[142]

The development of immunity passports also risks "alleviating the duty on governments to adopt policies that protect economic, housing, and health rights across society by providing an apparent quick fix."[143] This intervention emphasizes movement control as the solution to pandemic containment rather than building resource capacity, both in terms of the provision of adequate testing and healthcare infrastructure as well as the financial support needed for those required to stay at home unable to work without immunity.

Finally, such passports, as platforms for immunity data owned by governments or private companies, could be expanded to include other health information in the future. This not only would result in the expansion of health surveillance infrastructure beyond the pandemic, but could serve as a source of future discrimination if used by employers as a requirement for future work.[144]

What requirements are needed to protect user privacy?

As with every intervention discussed in this report, the use of such passports needs to be legal, necessary, and proportionate under international human rights law. There is no legal precedent for this, nor has this technology—for the reasons stated above—been proven as sufficiently necessary or proportionate to warrant implementation.[145] Therefore, such an intervention should not be pursued and resources focused elsewhere, into underfunded healthcare systems and communities most affected by the virus, the improvement of testing infrastructure, and to current gaps that technology can fill in the current healthcare infrastructure as identified by public health professionals and those working on the front lines.

If, however, through data-driven and evidence-based research such an intervention did become viable (a very unlikely outcome), then an immunity

[142] Ibid.; Bhandari and Moore, "Immunity Passports"; Mullin, "Immunity Passports;" Govind Persad and Ezekiel J. Emanuel, "The Ethics of COVID-19 Immunity-Based Licenses ('Immunity Passports')," JAMA 323, no. 22 (May 6, 2020): 2241-2242, https://doi.org/10.1001/jama.2020.8102.

[143] Quote from Phelan, "Immunity Passports." Also noted in Bhandari and Moore, "Immunity Passports."

[144] Aggarwal and Tackett, "Digital Health Certificates," 9-10; Bhandari and Moore, "Immunity Passports"; Kofler and Baylis, "Ten Reasons."

[145] Renieris, Bucher, and Smith, "Dangers."

certification program will require strong standards for testing, certification, renewal, and the storage of test results and associated health data. As Hall and Studdert note, “To be fair and effective, programs will need consensus standards for acceptable sensitivity and specificity of the tests, and systems for gathering test results to aid research and surveillance. Appropriately regulated, a certification program could actually reduce testing abuse that might otherwise occur.”[146] Data stored as part of any kind of certification process also needs to be subject to the same regulatory frameworks above in order to protect individual privacy and prevent its abuse by law enforcement.

Immunity passports also raise the need for greater protections against employment discrimination. If employers start mandating COVID-19 screening tests or proof of immunity to return to work, for example, strong anti-discrimination protections need to be in place to ensure that such requirements do not disproportionately impact some workers over others. The Americans with Disabilities Act (ADA) is cited as the most relevant legislation in this case, but whether immunity or risk of infection would constitute a “disability” as defined in the statute is up for debate.[147] As Henry T. Greely, Professor of Law and Director of the Stanford Center for Law and the Biosciences also points out, while the Equal Employment Opportunity Commission has issued COVID-19 guidelines for employers, the “direct threat” exception in the ADA only applies to those with symptoms or confirmed infection.[148]

[146] Hall and Studdert, “Immunity Certification.”

[147] Henry T. Greely, “First Opinion: Practical and ethical conundrums behind COVID-19 ‘immunity certificates,” Boston.com, April 11, 2020, https://www.boston.com/news/health/2020/04/11/first-opinion-covid-19-immunity-certificates-practical-and-ethical-conundrums; Mullin, “Immunity Passports.”

[148] Greely, “Conundrums”; “Pandemic Preparedness in the Workplace and the Americans with Disabilities Act,” U.S. Equal Employment Opportunity Commission, last updated March 21, 2020, https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act.

03 //

EXISTING REGULATORY FRAMEWORKS

03 //

EXISTING REGULATORY FRAMEWORKS

Applicable U.S. Data Privacy Regulations: A Snapshot

Given the privacy concerns raised by this suite of technological interventions, what regulatory frameworks exist to govern them? This proves to be a complicated question that many legal experts, privacy professionals, and human rights advocates are grappling with as application development, and the spread of the virus, continue apace. U.S. law is struggling to catch up, as it lacks any comprehensive, federal data privacy legislation equivalent to the European Union's General Data Protection Regulation (GDPR), implemented in 2018 and widely considered to be the current global "gold standard" for privacy regulation.[149] Instead, the U.S. has a patchwork of regulations that cover different types of user information in different ways depending on the jurisdiction in which the application lies, the type of data collected, and the type of company that holds it.[150] The following discussion briefly outlines some of the relevant legislation that applies to these technologies, as discussed by legal and privacy experts, as well as the COVID-19-specific legislation proposed to supplement them.[151]

[149] For this and a discussion of its limits, as well as the limits of individualized approaches to data governance, see Elizabeth Renieris, "The future of data governance," Medium, April 13, 2020, https://medium.com/berkman-klein-center/the-future-of-data-governance-c5723c38d70a.

[150] For a concise snapshot of such a patchwork see: Nuala O'Connor, "Reforming the U.S. Approach to Data Protection and Privacy," Council on Foreign Relations, January 30, 2018, https://www.cfr.org/report/reforming-us-approach-data-protection.

[151] Given the number of laws potentially applicable to the technologies discussed in the report, only the most commonly referenced are discussed here. A full analysis of all of the applicable laws is beyond the scope of this report. For a more detailed analysis of those relevant to contact tracing, see Kahn, Digital Contact Tracing, 75-94.

Federal Trade Commission Act, Section 5: Without comprehensive federal legislation, user data collected by applications and third parties are governed by the privacy policies and user agreements set forth by the individual companies collecting the data. The enforcement body responsible for assessing whether a company is adhering to its privacy policy is the Federal Trade Commission (FTC), with its enforcement of "unfair or deceptive practices" under Section 5.[152] While the FTC is designed as a consumer protection body, it has been playing a privacy oversight role in the last few years in order to ensure that consumer privacy is maintained.[153] The FTC would only be responsible for ensuring that a company was operating in accordance with its privacy policy, which would require the privacy policy itself to be strong enough to ensure adequate data protections.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA governs the collection and distribution of health information, yet it applies only to what the Department of Health and Human Services (HHS) calls "covered entities" such as health care providers, plans, and clearinghouses that store personal health information and their "business associates" (an entity hired or contracted by and therefore acting on behalf of a covered entity).[154] The Office of Civil Rights at HHS has also issued notification of discretionary enforcement of the HIPAA Privacy Rules and sharing of COVID-related data with public health authorities during the pandemic.[155] The HIPAA Rules do not apply to direct-to-consumer information sharing, therefore health or personal information collected by companies not defined as "covered entities" fall outside these regulations.[156] The COVID-19 data protection bills introduced into Congress (discussed below) aim at addressing data not covered by HIPAA.

[152] O'Connor, "Reforming the U.S. Approach."

[153] See Caitlin Potratz Metcalf's comments in Natasha Lomas, "What are the rules wrapping privacy during COVID-19?" TechCrunch, March 20, 2020, https://techcrunch.com/2020/03/20/what-are-the-rules-wrapping-privacy-during-covid-19/.

[154] "Who must comply with HIPAA privacy standards?" U.S. Department of Health and Human Services, last reviewed July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/faq/190/who-must-comply-with-hipaa-privacy-standards/index.html#:~:text=As%20required%20by%20Congress%20in,financial%20and%20administrative%20transactions%20electronically.

[155] "Notification of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19, 45 CFR Parts 160 and 164." U.S Department of Health and Human Services, April 2, 2020, https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-hipaa.pdf

[156] HHS has guidelines for application developers: "Health App Use Scenarios & HIPAA." U.S Department of Health and Human Services Office for Civil Rights, February 2016, https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html.

California Consumer Privacy Act (CCPA): Residents of California have greater data protections under the CCPA, which was passed in 2018 and went into effect in January 2020 with enforcement starting in July. Protections include the mandatory disclosure of what data are collected from consumers and the scope of their use, the right for the consumer to delete or opt-out of their data being sold to third parties, and the right to non-discrimination for exercising one's rights under the CCPA.[157] The law is mainly targeted at data brokers and does not apply to government entities or nonprofit organizations.[158] While this law is unprecedented and largely serves as a model for future federal privacy regulation, legal experts and privacy advocates note that it could go further by adding protections such as an expansion of private right of action and an opt-out default.[159]

To address some of these concerns, Californians for Consumer Privacy has secured the California Privacy Rights Act (CPRA) a slot on the ballot in November 2020, which would amend and add new provisions to the CCPA. Such amendments include the addition of a "sensitive data" category, the right to correct one's data and to a data minimization policy, expansion of a user's private right of action, as well as the establishment of a new enforcement body.[160]

While these existing entities offer some protections, the privacy of user data is still largely contingent on strong user agreements, privacy policies,

[157] "California Consumer Privacy Act," Office of the Attorney General of California, accessed July 19, 2020, https://oag.ca.gov/privacy/ccpa; California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100-1798.199 (2018).

[158] Ibid., Sara Morrison, "California's new privacy law, explained," Vox Recode, December 30, 2019, https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained.

[159] "California Legislature Caves to Big Tech Pressure Again and Undermines Consumer Privacy Rights," ACLU of Northern California, May 16, 2019, https://www.aclunc.org/news/california-legislature-caves-big-tech-pressure-again-and-undermines-consumer-privacy-rights; Morrison, "New Privacy Law"; Adam Schwartz et al., "Consumer Data Privacy in California: 2019 Year in Review," Electronic Frontier Foundation, December 31, 2019, https://www.eff.org/deeplinks/2019/12/year-review-consumer-data-privacy-california.

[160] For a full list see: Jim Halpert, Lael Bellamy, and Marco Berrios, "CPRA analysis: The 'good' and 'bad' news for CCPA-regulated 'businesses,'" IAPP, May 5, 2020, https://iapp.org/news/a/cpra-analysis-the-good-and-bad-news-for-ccpa-regulated-businesses/; Jerel Pacis Agatep, "The California Privacy Rights Act ('CPRA') Headed to the November 2020 Ballot," National Law Review, June 30, 2020, https://www.natlawreview.com/article/california-privacy-rights-act-cpra-headed-to-november-2020-ballot; Jeremy Greenberg, "CCPA 2.0? A New California Ballot Initiative is Introduced," Future of Privacy Forum, September 26, 2019, https://fpf.org/2019/09/26/ccpa-2-0-a-new-california-ballot-initiative-is-introduced/.

and the “good will” of the tech companies collecting it. To fill this gap, a few bills have been introduced in (but not passed by) Congress that seek to regulate personal information and health data collected by these new technologies that fall beyond HIPAA’s purview. These bills, and their benefits and drawbacks, are summarized below.

Federal Legislation Introduced for COVID-19 Data

In an effort to strengthen privacy protections for user data collected for the purposes of COVID-19 mitigation, the following bills have been introduced to Congress during the pandemic:

The Covid-19 Consumer Data Protection Act of 2020,[161] proposed by Senate Republicans, and the Public Health Emergency Privacy Act (PHEPA),[162] put forward by House and Senate Democrats, were both introduced in May. As both the EFF and the Future of Privacy Forum point out in detailed analyses of the bills, the PHEPA would introduce more comprehensive privacy protections for U.S. consumers and is, therefore, the preferred approach of privacy advocates.[163] Both bills would mandate data minimization (collection of only what is necessary and proportional); express consent; sunsetting of the data post-pandemic; and would increase transparency through collection notification, mandatory deletion, and enforcement (albeit through different bodies). The Republican-backed bill, however, would preempt state laws, cutting back existing protections already in place across the country, and include exceptions for employers, allowing employers to mandate the use of screening tools for its workers. These factors, in addition to the broader scope of the Democrat-backed bill, make it the primary choice of leading privacy advocates.[164]

[161] U.S. Congress, Senate, Covid-19 Consumer Data Protection Act of 2020, S 3663, 116th Cong., 2nd sess., introduced in Senate May 7, 2020, https://www.congress.gov/116/bills/s3663/BILLS-116s3663is.pdf.

[162] U.S. Congress, House, Public Health Emergency Privacy Act, S 3749, 116th Cong., 2nd sess., introduced in House May 14, 2020, https://www.congress.gov/116/bills/s3749/BILLS-116s3749is.pdf.

[163] Adam Schwartz, "Two Federal COVID-19 Privacy Bills: A Good Start and a Misstep,” Electronic Frontier Foundation, May 28, 2020, https://www.eff.org/deeplinks/2020/05/two-federal-covid-19-privacy-bills-good-start-and-misstep; Pollyanna Sanderson, Stacey Gray, and Katelyn Ringrose, "Newly Released COVID-19 Privacy Bills Would Regulate Pandemic-Related Data,” Future of Privacy Forum, May 15, 2020, https://fpf.org/2020/05/15/newly-released-covid-19-privacy-bills-would-regulate-pandemic-related-data/.

[164] For full analysis of the benefits and drawbacks of each bill see: Schwartz, “Privacy Bills”; Sanderson, Gray, and Ringrose, "COVID-19 Privacy Bills”; Paul Schwartz, “Illusions of Consent.”

Following the announcement of the Google / Apple API, the Exposure Notification Privacy Act was introduced in June 2020.[165] A bipartisan bill aimed at protecting data held by exposure notification services such as apps or websites, it applies to companies running such services, mandates collaboration with public health officials, requires "affirmative express consent," as well as transparency regarding the use and effectiveness of such services in addition to their privacy policies. It also introduces purpose limitations (for public health use only, barring commercial purposes), data minimization, and deletion and security requirements for the data held.[166] It leaves enforcement to the FTC and State Attorneys General, and does not preempt any other state laws.

The most recent bill, introduced by House Democrats in July, is the Secure Data and Privacy for Contact Tracing Act of 2020,[167] which would provide CDC grant funding to states and tribal governments for the use of digital contact tracing tools if they comply with certain data protections. These protections include voluntary affirmative consent and disclosure of use, purpose and use limitations, required deletion 30-days after the pandemic is declared over, encryption requirements, as well as the need for independent security assessments. HIPAA also applies to the data collected by digital tools funded through this bill. Ashkan Soltani, Distinguished Fellow at Georgetown University and former Chief Technologist of the Federal Trade Commission, reportedly endorses this bill as well.[168]

In addition, there are two other pandemic-related bills worth noting that include data privacy protections. The Coronavirus Containment Corps Act,[169] a bill introduced in the Senate in June by Democrats led by Sen. Elizabeth

[165] U.S. Congress, Senate, Exposure Notification Privacy Act, S 3861, 116th Cong., 2nd sess., introduced in Senate June 1, 2020, https://www.congress.gov/116/bills/s3861/BILLS-116s3861is.pdf.

[166] Nicole Su, "Exposure Notification Privacy Act: Bipartisan Bill Introduced to Regulate Covid-19 Contact Tracing Apps," National Law Review, June 18, 2020, https://www.natlawreview.com/article/exposure-notification-privacy-act-bipartisan-bill-introduced-to-regulate-covid-19.

[167] U.S. Congress, House, Secure Data and Privacy for Contact Tracing Act of 2020, HR 7472, 116th Cong., 2nd sess., introduced in House July 1, 2020, https://www.congress.gov/116/bills/hr7472/BILLS-116hr7472ih.pdf.

[168] Rep. Jackie Speier, "Reps Speier, DeGette, and Dingell Introduce Legislation to Protect Privacy in Contact Tracing Technology," Press Release, (July 1, 2020), https://speier.house.gov/press-releases?ID=EA0CED08-6BED-463A-9647-4D4F0404BCB8.

[169] U.S. Congress, Senate, Coronavirus Containment Corps Act, S 3848, 116th Cong., 2nd sess., introduced in Senate June 1, 2020, https://www.congress.gov/116/bills/s3848/BILLS-116s3848is.pdf.

Warren, outlines a national strategy for contact tracing that would include protections such as minimization, anonymization, and restrictions on data sharing collected through mobile contact-tracing applications.

Senator Warren also introduced the Equitable Data Collection and Disclosure on COVID-19 Act,[170] which would mandate that HHS publish COVID-19 testing, treatment, and outcome data disaggregated by race, ethnicity, disability status, and other demographic information to gain a better picture of how COVID-19 is affecting marginalized communities nationwide. Such data collection would enable increased visibility of the impacts on communities of color, increase funding to improve data collection infrastructure, and focus resources to meet the needs of those most affected by the virus.[171]

All six bills have only been introduced, however, and have not made it further in Congress at the time of writing.

[170] U.S. Congress, Senate, Equitable Data Collection and Disclosure on COVID-19 Act, S 3850, 116th Cong., 2nd sess., introduced in Senate June 1, 2020, https://www.congress.gov/116/bills/s3850/BILLS-116s3850is.pdf.

[171] See also: Sen. Elizabeth Warren, “Senator Warren Introducing Bicameral Legislation to Require Federal Government to Collect and Report Coronavirus Demographic Data -- Including Race and Ethnicity.” Press Release, (April 14, 2020), https://www.warren.senate.gov/newsroom/press-releases/senator-warren-introducing-bicameral-legislation-to-require-federal-government-to-collect-and-report-coronavirus-demographic-data_--including-race-and-ethnicity

04 //

CONCLUSIONS

04 //

CONCLUSIONS

This report has outlined the goals, function, and concerns raised by four types of technology that have been circulating in the U.S. as potential tools for COVID-19 mitigation. Each type, as well as the difference in approaches within them, present unique challenges and therefore unique requirements and recommended courses of action. While an overview of recommendations for each technology is provided in this report, attention should be devoted to the existing research and expert recommendations on the individual technology being considered. To facilitate this effort, a list of key resources is provided at the end of this report, in addition to the citations included throughout, to facilitate decision-making efforts.

Despite these differences, however, some key themes and, thus, key take-aways to consider emerge when weighing where and how the power of technology should be mobilized in the current health crisis. Four conclusions from the research are presented below, followed by broad recommendations for the use of technology for pandemic response.

First, as many of the technologists and experts featured in this report have noted, technology cannot be considered a "panacea" or "silver bullet" for COVID-19 mitigation.[172] **Any technological intervention will have to function as one component of a larger public health response, one that needs adequate resources and strong leadership to succeed.** Containment of the pandemic will be a result of a coordinated national response that delivers clear information and protocols to the general public, driven by public health expertise and epidemiological evidence. While technology might have a role to play, it is in facilitating this effort rather than generating data of questionable utility. At the moment, the availability of accurate, widespread, and rapid testing at scale; comprehensive support for the tracing, treatment, and isolation of cases; and an adequate supply of

[172] This was noted widely within the resources cited in this report. A selection include: Bourdeaux, Gray, and Grosz, "Human-Centered Tech"; Daskal et al., "Privacy"; Schwartz, "Protecting Privacy."

resources such as ventilators, masks, and PPE to the healthcare facilities that need it are just a few of the items required in the U.S. for such technologies to be beneficial, if they are even taken up on a large scale.

Second, **technological interventions must be evidence-based and led by the needs of public health authorities, healthcare professionals, and others working at the center of emergency response.** Exposure notification tools and immunity passports lack sufficient evidence to support their use and have a high likelihood of exacerbating, rather than diminishing, the disparate effects of the pandemic on communities of color. While aggregated location data has epidemiological support for its use in certain cases, significant safeguards for the data as well as full disclosure of its analysis and use must be made to account for the limited representativeness of the data. Symptom-tracking applications also have epidemiological support, especially when used in a clinical study context, but present similar concerns regarding representativeness. The lack of representativeness of the data—and who it represents—is a strong argument for significantly limiting its use to certain cases only with the proper safeguards, otherwise to not use it at all. If public health decisions and policy are designed solely based on data with partial representation, for example, outcomes could be misleading and increase harm to already marginalized communities.

Third, **technological interventions currently risk exacerbating, rather than counteracting, existing disparities in pandemic impact.** All four of the technologies featured in this report concentrate risk of harm in low-income groups and communities of color, due to their reliance on smartphones, the (potential lack of) representativeness of the data, as well as the likelihood of mission creep, increased surveillance, and chance of appropriation by law enforcement. As Mary L. Gray, Senior Researcher at Microsoft, put it plainly, "today's tech approaches to COVID-19 exacerbate the systemic racism and health disparities that have given the pandemic its grotesque shape in our country—because they ignore them."[173] Rather than be used to actively counteract unequal access to healthcare, the provision of adequate testing, and treatment for communities of color, such interventions have the potential to reinscribe such divisions through their very design.

Finally, it is important to note that **the reinscription of racialized and classed bias in technology, the law, and public health has deep historical precedent.** As such, today's technological responses in the name of public health must be set within the context of a long history of legalized

[173] Mary Gray, "'Colorblind' Tech is Killing Us: Why COVID-19 Tech Must Focus on Equity," Medium, June 15, 2020, https://medium.com/berkman-klein-center/colorblind-tech-is-killing-us-why-covid-19-tech-must-focus-on-equity-9cd2b67cf84c.

discrimination, medical experimentation, and the expansion of surveillance on Black lives and other poor and working people of color, as well as the racial bias rampant in purportedly neutral technologies today.[174] Set within the current health crisis, Michele Goodwin, Founding Director of the Center for Biotechnology and Global Health Policy at UC Irvine School of Law, reminds us that "protecting the public's health has at times served as a proxy for bias, discrimination, and nativism."[175] The turn to technology and unreliable data for pandemic response, even if well intentioned, could serve to entrench these longstanding biases, already evident in the patterns of pandemic impact. As historian Rosemary Taylor points out, "pandemics can inspire forgetting as well as remembering," as governments as well as their citizens often resort to familiar response tactics despite their proven ineffectiveness or unnecessary costs.[176] This moment provides us with an opportunity to think and act differently, to counteract the hierarchical structures that shape the society in which we live and our pre-programmed responses to it.

174. Ruha Benjamin, Race After Technology: Abolitionist Tools for the New Jim Code (Medford MA: Polity Press, 2019); Browne, Dark Matters; Richardson, Nkonde, and Williams, "Surveilling Black Lives"; Richard Rothstein, The Color of Law: A Forgotten History of How Our Government Segregated America (New York: Liveright Publishing Corporation, 2017); Harriet A. Washington, Medical Apartheid: The Dark History of Medical Experimentation on Black Americans from Colonial Times to the Present (New York: Harlem Moon, 2006). This is merely a selection of work describing this history.

175. Michele Goodwin and Erwin Chemerinsky, "No Immunity: Race, Class, and Civil Liberties in Times of Health Crisis," Harvard Law Review 129 (2016): 956-96, http://cdn.harvardlawreview.org/wp-content/uploads/2016/02/956-996-Online.pdf; See also Michele Goodwin, Jennifer Granick, and Emerson Sykes, "97: A COVID-19 Balancing Act: Public Health and Privacy," April 30, 2020, on At Liberty, produced by the ACLU, podcast, 27:58, https://www.aclu.org/podcast/covid-19-balancing-act-public-health-and-privacy-ep-97.

176. Rosemary Taylor, "History Lessons: Can We Learn from the Past?" SSRC Items, July 16, 2020, https://items.ssrc.org/covid-19-and-the-social-sciences/democracy-and-pandemics/history-lessons-can-we-learn-from-the-past/.

05 //

RECOMMENDATIONS

05 //

RECOMMENDATIONS

With these four conclusions in mind, we make the following recommendations:

1. **Refocus technological skills and expertise on addressing existing bottlenecks in the public health and logistics infrastructure, as identified by frontline health workers, public health officials, epidemiologists, and supply chain professionals facilitating the response effort.**[177] Examples include the provision of secure databases, communication tools, and record storage for contact tracers;[178] the design of case management tools to connect quarantined individuals with necessary health information, financial and legal support, and eviction protections in secure ways;[179] and improvements to secure data storage and sharing across healthcare facilities, in order to replace obstacles such as the fax machine.[180]

2. **Redirect and reinvest resources into such solutions, underfunded and under-resourced health facilities, and into communities most affected by the virus.** Rather than investing in interventions with questionable utility, resources should be targeted at providing impacted communities with equitable testing and treatment, as well as the financial and social support needed to quarantine and recover without fear of job loss or eviction. Resources, in both the immediate and distant future, should be aimed at changing—rather than reinforcing—the very structural conditions that created the disproportionate impact of the pandemic in the first place.

3. **Ensure that interventions are evidence-based, use verifiable data, and are driven by the public health needs of affected communities.**

[177] Bourdeaux et al., "Contact tracing."

[178] Bourdeaux, Gray, and Grosz, "Human-Centered Tech."

[179] Bourdeaux et al., "Contact tracing."

[180] Sarah Kliff and Margot Sanger-Katz, "Bottleneck for U.S. Coronavirus Response: The Fax Machine," New York Times, July 13, 2020, https://www.nytimes.com/2020/07/13/upshot/coronavirus-response-fax-machines.html.

Many of the current technologies proffered for pandemic mitigation lack sufficient evidence to justify their use, or rely on self-reported information unverified by a public health authority. Rather than put energy and resources toward these efforts, application design and data collection should be focused on data that affected communities, epidemiologists, data experts, and public health authorities say are needed, such as data disaggregated by race, ethnicity, and tribal affiliation to highlight where resources should be focused.[181] Such data, however, should always be collected in collaboration with and owned by the communities and tribal nations contributing that data.[182]

4. **Technological interventions, if used, must be accountable to the communities they affect.** Communities hit hardest by the virus should be consulted in the design, review, and evaluation of proposed interventions, with mechanisms built-in for sustained, meaningful engagement, feedback, and community oversight.[183] As mentioned above, as many data experts and scholars have made clear, COVID-19 data should always be collected, controlled, used, and shared in collaboration and partnership with those communities affected by and with rights to the data.[184] To that end, concrete mechanisms for participation need to be incorporated into every phase of project development and implementation, as well as oversight to ensure effectiveness and mitigation of harm or disparate impact.[185]

5. **Interventions should be accessible to all individuals regardless of disability or immigration status, gender identity, access to internet or housing, or other barriers to participation.** Technological interventions and the data they collect should never be permitted for use by law or immigration enforcement bodies, nor should they ever be made a requirement for treatment, access to services or spaces, or a condition of employment. User interfaces themselves must also be made accessible by providing applications and associated information in

[181] Aletha Maybank, “Why racial and ethnic data on COVID-19’s impact is badly needed,” American Medical Association, April 8, 2020, https://www.ama-assn.org/about/leadership/why-racial-and-ethnic-data-covid-19-s-impact-badly-needed; Stephanie Russo Carroll et al., “Indigenous Data in the Covid-19 Pandemic: Straddling Erasure, Terrorism, and Sovereignty,” SSRC Items, June 11, 2020, https://items.ssrc.org/covid-19-and-the-social-sciences/disaster-studies/indigenous-data-in-the-covid-19-pandemic-straddling-erasure-terrorism-and-sovereignty/; Watson-Daniels et al., “Movement Pulsecheck,” 25-6.

[182] Russo Carroll et al., “Indigenous Data”; Watson-Daniels et al., “Movement Pulsecheck,” 22-4.

[183] Brighthive and Future of Policy Forum, “Playbook.”

[184] Russo Carroll et al., “Indigenous Data”; Watson-Daniels et al., “Movement Pulsecheck,” 22-4.

[185] Brighthive and Future of Policy Forum, “Playbook.”

multiple languages, providing alternatives for the visually impaired, or allowing for the use of preferred name and non-binary pronouns in the user interface, as many gender non-conforming and trans-identifying people might have names and pronouns that do not match their legal documentation. The privacy and security of such data is also of utmost importance (addressed below), as the inadvertent sharing of health information could put many already marginalized individuals at even greater risk of discrimination or retribution.

6. **Comprehensive federal data privacy legislation is needed, including strong mechanisms and resources for enforcement.** Within the fragmented data legislation landscape in the U.S., the protection of any kind of personally identifiable information largely relies on the goodwill of the companies or governments collecting such data or places the burden on the user to take action. The type of data collected for COVID-19 mitigation and research, as with any health data, is incredibly sensitive with great consequence if misused, breached, or acquired by law enforcement through mission creep. In the face of such stakes, the research presented here highlights the need for comprehensive data privacy legislation on the federal level in order to ensure such data is proactively protected. Such legislation should include strong enforcement mechanisms, as well as the resources and staffing required to support and expand the enforcement capacity of the assigned entities.[186]

7. **Any user data that is collected must still be subject to privacy-by-design standards, including limitations as to its purpose and use.** Data collected through emerging pandemic mitigation tools need adequate safeguards in place, such as clear purpose limitations, strong privacy policies and user agreements, and oversight over third-party access. Decision-makers should consult privacy advocates for the appropriate safeguards required for the particular application or use case of the data being considered. Regardless of the approach taken, however, applications, tools, and the data they collect should be used for pandemic purposes only and be barred from use by law or immigration enforcement; should never be made a requirement for employment, access to certain spaces, treatment, or for social services of any kind; and should also be barred from use for commercial purposes.

In addition, mirroring the list of requirements privacy advocates recommend for exposure-notification tools above, the following data protections should also be in place:

[186] Serge Egelman, in discussion with the author, August 10, 2020.

- Affirmative consent and opt-in for data collection and use, acquired separately for each type of data collected.[187]

- Clear and concise user agreements and privacy policies outlining data use, methodology, access, and dissemination, ideally in a standardized format.[188]

- Adherence to privacy-by-design principles including data minimization, deletion requirements, anonymization, and encryption, tailored to the purpose at hand.[189]

- Limitations on data retention and expiration of the tools themselves once the state of emergency has been lifted.[190]

- Individual user rights for editing, withholding, and deletion of data, as well as the possibility of recourse through private action.[191]

- Third-party assessment and oversight of the tools in use, including open source code for external privacy and security review as well as recurring ethics and impact assessments that include representation from communities providing their data.[192]

[187] Crocker et al., “Challenge of Proximity Apps”; Hoffman-Andrews and Crocker, "Protect Privacy”; Human Rights Watch, “Q&A.”

[188] Daskal et al., “Privacy”; Egelman, interview. For an earlier piece on this, see Zeynep Tufekci, “We Already Know How to Protect Ourselves from Facebook,” New York Times, April 9, 2018, https://www.nytimes.com/2018/04/09/opinion/zuckerberg-testify-congress.html

[189] Brighthive and Future of Policy Forum, “Playbook”; Gillmor, “Principles”; Human Rights Watch, “Q&A.”

[190] Daskal et al., “Privacy”; Lisa Hayes et al., “COVID-19 Webinar Series: Gaps in U.S. Privacy and Surveillance Law Laid Bare by Coronavirus,” Webinar hosted by the Center for Democracy and Technology, April 30, 2020, https://www.youtube.com/watch?v=-gy-qSFpTwc&feature=youtu.be.

[191] Hoffman-Andrews and Crocker, "Protect Privacy”; Schwartz, “Privacy in California.”

[192] Brighthive and Future of Policy Forum, “Playbook”; Gillmor, “Principles,” 10.

ACKNOWLEDGMENTS

The author would like to thank Tessa Alexanian, Privacy and Security Advisor for Covid Watch; Deirdre Mulligan, Associate Professor in the UC Berkeley School of Information; and Serge Egelman, Research Director of the Usable Security & Privacy Group at the International Computer Science Institute for sharing their insights on these important issues. This research was funded by the Human Rights Center at UC Berkeley and was advised by Brandie Nonnecke, Director of the CITRIS Policy Lab at UC Berkeley. The views expressed here and any errors are the author's alone.

ADDITIONAL RESOURCES

The following list is a selection of resources that provide a deeper dive into the issues addressed in the report. This is not a comprehensive list, but a supplement to the information provided above.

COVID-19 Data Collection Broadly (not specific to or featuring multiple technologies)

"BKC Policy Practice: Digital Pandemic Response Program," *Berkman Klein Center for Internet and Society at Harvard University*. Last updated August 7, 2020. https://cyber.harvard.edu/programs/bkc-policy-practice-digital-pandemic-response.

"Collecting & Sharing Geo-Located Data in Crisis Situations: Decision-Making Tools for Practitioners." *Scientific Responsibility, Human Rights and Law Program of the American Association for the Advancement of Science*, 2019. https://www.theengineroom.org/wp-content/uploads/2019/12/AAAS-Decision-Trees.pdf.

"COVID-19 Privacy and Data Protection Resources." *Future of Privacy Forum*. Last updated May 5, 2020. https://sites.google.com/fpf.org/covid-19-privacy-resources.

"Mobile Location Data and Covid-19: Q&A." *Human Rights Watch,* May 3, 2020. https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa#.

Stanley, Jay and Jennifer Stisa Granick. "The Limits of Location Tracking in an Epidemic." *ACLU*, April 8, 2020. https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic.

Watson-Daniels, Jamelle, Yeshimabeit Milner, Nicole Triplett, Irene Headen, Dominique Day, Zinzi Bailey, Meme Styles, et al. "Data for Black Lives COVID-19 Movement Pulsecheck and Roundtable Report." *Data for Black Lives.* April 2020. d4bl.org/reports.html.

Digital Contact Tracing Tools

Bourdeaux, Margaret, Mary L. Gray, Mona Sloan, Peggy Hamburg, Andrew McLaughlin, and Jonathan Zittrain. “Contact tracing: what it is, how it works, how tech can help.” Online panel hosted by COVID-19 Technology Task Force, June 17, 2020, https://techcrunch.com/2020/06/16/j oin-us-june-17-for-a-live-discussion-on-covid-19-contact-tracing-and-safe-reopening-strategies/

Crocker, Andrew, Kurt Opsahl, and Bennett Cyphers. “The Challenge of Proximity Apps For COVID-19 Contact Tracing.” *Electronic Frontier Foundation*, April 10, 2020. https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing.

“Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing.” *World Health Organization*, May 28, 2020. https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

Gillmor, Daniel Kahn. “Principles for Technology-Assisted Contact Tracing.” *ACLU*, April 16, 2020. https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing.

Kahn, Jeffrey (ed.) and the Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies. *Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance.* Baltimore: Johns Hopkins University Press, 2020.

Landau, Susan, Christy E. Lopez, and Laura Moy. “The Importance of Equity in Contact Tracing.” *Lawfare,* May 1, 2020. https://www.lawfareblog.com/importance-equity-contact-tracing.

“Responsible Data Use Playbook for Digital Contact Tracing.” *Brighthive and the Future of Privacy Forum.* 2020. https://playbooks.brighthive.io/contact-tracing/.

Aggregated Location Data

Azarmi, Mana and Andy Crawford. “Use of Aggregated Location Information and COVID-19: What We’ve Learned, Cautions about Data Use, and Guidance for Companies.” *Center for Democracy and Technology,* 2020. https://cdt.org/wp-content/uploads/2020/05/2020-05-29-Use-of-Aggregated-Location-Information-and-Covid-19.pdf.

Balsari, Satchit, Caroline Buckee, and Tarun Khanna. "Which Covid-19 Data Can You Trust?" *Harvard Business Review,* May 8, 2020. https://hbr.org/2020/05/which-covid-19-data-can-you-trust.

Hoffman-Andrews, Jacob and Andrew Crocker. "How to Protect Privacy When Aggregating Location Data to Fight COVID-19." *Electronic Frontier Foundation*, April 6, 2020. https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19.

Toh, Amos. "Big Data Could Undermine the Covid-19 Response." *Wired Magazine,* April 12, 2020. https://www.wired.com/story/big-data-could-undermine-the-covid-19-response/.

Immunity Passports

Aggarwal, Naman M. and Carolyn Tackett. "The impact of COVID-19 digital health certificates." *Access Now*, July 2020. https://www.accessnow.org/cms/assets/uploads/2020/07/Impact-COVID-19-digital-health-certificates.pdf.

Bhandari, Esha and ReNika Moore. "Coronavirus 'Immunity Passports' are not the Answer." *ACLU,* May 18, 2020. https://www.aclu.org/news/privacy-technology/coronavirus-immunity-passports-are-not-the-answer/.

Greely, Henry T. "First Opinion: Practical and ethical conundrums behind COVID-19 'immunity certificates." *Boston.com,* April 11, 2020. https://www.boston.com/news/health/2020/04/11/first-opinion-covid-19-immunity-certificates-practical-and-ethical-conundrums.

Hall, Mark A. and David M. Studdert. "Privileges and Immunity Certification During the Covid-19 Pandemic." *JAMA* 323, no. 22 (May 6, 2020): 2243-2244. https://doi.org/10.1001/jama.2020.7712.

Kofler, Natalie and Françoise Baylis. "Ten reasons why immunity passports are a bad idea." *Nature* 581 (May 21, 2020): 379-81. https://media.nature.com/original/magazine-assets/d41586-020-01451-0/d41586-020-01451-0.pdf.

Phelan, Alexandra L. "COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges." *The Lancet 395*, no. 10237 (May 4, 2020): 1595-1598. https://doi.org/10.1016/S0140-6736(20)31034-5.

ABOUT

The CITRIS Policy Lab is a sub-organization of the Center for Information Technology Research in the Interest of Society and the Banatao Institute (CITRIS), headquartered on the UC Berkeley campus. Founded in 2001, CITRIS leverages expertise on the campuses of UC Berkeley, UC Davis, UC Merced, and UC Santa Cruz to develop technology applications with societal and economic benefits. The CITRIS Policy Lab was established in 2018 to support interdisciplinary technology policy research analyzing technology capabilities and their implications for society. Through its collaboration with public and private sector stakeholders, the CITRIS Policy Lab addresses core questions regarding the role of formal and informal regulation in promoting innovation and amplifying its positive effects on society.

The Human Rights Center at the University of California, Berkeley, School of Law conducts research on war crimes and other serious violations of international humanitarian law and human rights. Using evidence-based methods and innovative technologies, we support efforts to hold perpetrators accountable and to protect vulnerable populations. We also train students and advocates to research, investigate, and document human rights violations and turn this information into effective action. We are guided by the need to listen to and support survivors, test innovative ideas, draw from multiple disciplines, use rigorous methods, and collaborate.