Remarks at Privacy + Security Academy

Privacy and Public/Private Partnerships in a Pandemic

Christine S. Wilson*
Commissioner, U.S. Federal Trade Commission

Virtual Event
May 7, 2020

* The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner. Many thanks to my Attorney Advisor, Robin Rosen Spector, for assisting in the preparation of these remarks.

I. Introduction

Good afternoon! Many thanks, Professor Solove, for inviting me to speak today. This event is one of the premier conferences on privacy issues, so I am pleased that Covid-19 has not derailed the gathering. But the pandemic has derailed the remarks I originally envisioned delivering. When I was first invited to speak, we were not discussing social distancing and toilet paper shortages. Instead, we were discussing draft privacy bills circulated by member of the U.S. Congress. At that time, I thought it would be useful – if not necessarily scintillating – to do a deep dive on federal preemption and private rights of action, two apparent stumbling blocks for privacy legislation. Then governments issued stay-at-home orders, this conference moved to a virtual space, and privacy issues related to the pandemic began to pepper the daily news. In keeping with the times, it seems more appropriate to discuss the pandemic-driven privacy challenges that governments and the private sector are facing today.

I plan to focus my remarks today on three topics. First, I will describe the proliferation of public/private partnerships to address the current pandemic. Second, I will identify the potential privacy risks from these partnerships. And third, I will provide some recommendations for how businesses and governments should work to mitigate these risks.

Before I dive in, I must give the standard disclaimer that the views I express here are my own and do not necessarily reflect those of the Federal Trade Commission or any other Commissioner.

II. Proliferation of Partnerships

It seems an understatement to say that we are living through historic times. In the United States alone, we have witnessed almost 1.2 million confirmed cases of Covid-19, and more than

seventy thousand people have succumbed to this disease.[1] Tragically, the worldwide numbers are far higher.[2] And billions of citizens around the globe are operating under shelter-in-place directives as governments grapple with how to stem the tide of infection and death.[3]

Many governments are turning to technology for assistance. The desire to use modern technology on a broad scale for the sake of public safety is not unique to this moment. Technology is intended to improve the quality of our lives, in part by enabling us to help ourselves and one another. Here in the United States, an organization called the National Partnership for Missing and Exploited Children coordinates with state and local authorities to send out Amber Alerts through privately owned wireless carriers. The goal of these alerts is to locate and recover abducted children safely. But this is just one example; the robust civil society and free market in the U.S. make partnerships between the private sector and government agencies commonplace.

These partnerships are not unique to the U.S. It is not surprising that we have seen a proliferation of such partnerships to address the challenges of this pandemic. These partnerships deploy government omnipotence and private sector omniscience to monitor and enforce

---

[1] Centers for Disease Control, Coronavirus Disease 2019 (COVID-19) (May 6, 2020) (reporting 1,193,814 cases and 70,802 deaths), https://www.cdc.gov/coronavirus/2019-ncov/cases-updates/cases-in-us.html.

[2] World Health Organization, Coronavirus disease 2019 (COVID-19) Situation Report – 107 (May 6, 2020) (reporting 3,588,733 confirmed cases and 247,503 deaths), https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200506covid-19-sitrep-107.pdf?sfvrsn=159c3dc_2.

[3] Prime Minister of India, PM's address to the nation on vital aspects relating to the menace of COVID-19, March 24, 2020 (putting more than 1.3 billion people on a 21-day lockdown), https://www.pmindia.gov.in/en/news_updates/pms-address-to-the-nation-on-vital-aspects-relating-to-the-menace-of-covid-19/; UK Government, PM address to the nation on coronavirus, March 23, 2020 (putting more than 66.5 million people on an indefinite lockdown, to be reviewed after three weeks), https://www.gov.uk/government/speeches/pm-address-to-the-nation-on-coronavirus-23-march-2020; Republic of South Africa Government Gazette, Disaster Management Act (57/2002) Amendment, March 25, 2020, https://www.gov.za/documents/disaster-management-act-regulations-address-prevent-and-combat-spread-coronavirus-covid-19 (putting more than 58 million people on a 21-day lockdown). Of other highly populous jurisdictions, most of the populations of the United States and the European Union, and much of Indonesia, Pakistan, Brazil, Nigeria, Russia, Mexico, Thailand and the Philippines, are under regional lockdowns.

quarantines and conduct contact tracing to mitigate the spread of this disease.[4] In fact, many view technology, particularly in the form of comprehensive contact tracing, as the key to safely easing quarantines and resuming normal economic and social life.[5] Notably, all of these efforts are fueled by extensive collection and analysis of sensitive data in connection with people's movements and health.

A word about contact tracing is warranted. Contact tracing is a time tested public health strategy, used to fight the spread of infectious diseases such as tuberculosis,[6] the 2014 Ebola outbreak and the 2003 SARS epidemic.[7] Traditionally, contact tracing is a labor-intensive effort, conducted manually by public health officials. It requires locating all individuals with whom an infected person has come into close contact. Experience teaches that contact tracing is an

[4] There have also been partnerships announced related to treatments, vaccines, and virus testing. For example, Amazon announced cornovirus testing lab for workers. Jay Greene, *Amazon developing coronanvirus testing lab for workers*, WASHINGTON POST (Apr. 4, 2020), https://www.washingtonpost.com/technology/2020/04/09/amazon-coronavirus-testing-lab/. And, NIH launched public/private partnerships to speed Covid-19 vaccine and treatment options. News Releases: NIH to launch public-private partnership to speed COVID-19 vaccine and treatment options (Apr. 17, 2020), available at: https://www.nih.gov/news-events/news-releases/nih-launch-public-private-partnership-speed-covid-19-vaccine-treatment-options.

[5] *See, e.g.*, Maryland Strong: Roadmap to Recovery (Apr. 24, 2020) (relies on contact tracing as part of plan to reopen economy), available at: https://governor.maryland.gov/wp-content/uploads/2020/04/MD_Strong.pdf; New York and Washington state also have contact tracing as an integral part of their reopening plans. Jesse McKinley, *Cuomo's N.Y. Reopening Plan*, NY TIMES (May 4, 2020) (Governor Cuomo stated he wants at least 30 working contact tracers per 100,000 residents); https://www.nytimes.com/2020/05/04/nyregion/coronavirus-reopen-cuomo-ny.html?action=click&module=Top%20Stories&pgtype=Homepage; Martin Kaste, *Washington State Builds Coronavirus Contact Tracing "Fire Brigade"* NPR (Apr. 22, 2020) (describing Washington's plan to use rigorous contact tracing to reopen the state); https://www.npr.org/sections/coronavirus-live-updates/2020/04/22/842119284/washington-state-builds-coronavirus-contact-tracing-fire-brigade. The American Enterprise Institute (AEI) think tank also issued a roadmap to reopening that includes large-scale contact tracing. AEI: National Coronavirus Response: A Road Map to Reopening, (Mar. 28, 2020), available at: https://www.aei.org/wp-content/uploads/2020/03/National-Coronavirus-Response-a-Road-Map-to-Recovering-2.pdf.

[6] Centers for Disease Control, Guidelines for the Investigation of Contacts of Persons with Infectious Tuberculosis, December 16, 2005, https://www.cdc.gov/mmwr/preview/mmwrhtml/rr5415a1.htm ("investigation of contacts and treatment of infected contacts is an important component of the U.S. strategy for TB elimination, second in priority to treatment of persons with TB disease").

[7] Alejandro De La Garza, *What is Contact Tracing? How will it be used for COVID-19*, TIME (Apr. 22, 2020), https://time.com/5825140/what-is-contact-tracing-coronavirus/.

effective solution when infection levels are relatively low.[8] Given the high levels of infection of Covid-19, people hope a high-tech solution, with widespread adoption, is viable.

Apple and Google recently announced a BlueTooth-based contact-tracing platform that has garnered global attention and been adopted in several countries.[9] Public health authorities have been invited to build apps for this platform. The network relies on BlueTooth rather than location to detect proximity to other devices and alert users if they have come into contact with infected individuals. Apple and Google have stated that the system will not collect personally identifiable information or user location data and have promised that those who share a diagnosis via the app will not have their identities disclosed to the companies or other users. The data will be used only by public health officials.

Similarly, Microsoft and the University of Washington announced a contact-tracing app, CovidSafe.[10] This app, according to news reports, will use the GPS location data in an infected person's phone to allow public health authorities to post alerts disclosing the locations visited by the person with Covid-19. Other individuals can then use the app to cross-reference the location data in their phones to determine if they were in that location at the same time.

These initiatives are new, so little is known about the kinds of information that will be collected, who will have access to it, with whom it will be shared, how long it will be retained,

---

[8] *Id.*; *see also* Ashkan Soltani, et al., *Contact-tracing apps are not a solution to the COVID-19 crisis*, BROOKINGS INSTITUTE (Apr. 27, 2020), available at: https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

[9] News Release: Apple-Google Partner on Covid-19 Contact-tracing Technology (Apr. 10, 2020), available at: https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology; Cat Zakrzewsky, *U.S. gears up for privacy debate as coronavirus phone monitoring expands globally*, WASHINGTON POST (May 4, 2020) (noting that Israel and Germany have adopted the Apple-Google technology), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/05/04/the-technology-202-u-s-gears-up-for-privacy-debate-as-coronavirus-phone-monitoring-expands-globally/5eaee1b788e0fa594778d848/?utm_campaign=wp_the_technology_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_technology202.

[10] Lisa Stiffler, *UW and Microsoft release contact-tracing aiming to battle COVID-19 while preserving privacy*, GEEKWIRE (Apr. 22, 2020), https://www.geekwire.com/2020/uw-microsoft-release-contact-tracing-app-aiming-battle-covid-19-preserving-privacy/.

and a host of other questions that we would typically ask. There are also important questions about the efficacy of these apps – studies assert that contact tracing via app may lack the superior accuracy of manual tracing and caution that these apps may be subject to manipulation for nefarious purposes.[11]

Other public/private partnerships employ technology to enforce stay-at-home orders. For example, the Covid-19 Mobility Data Network draws on mobile device data from users of Facebook, Camber Systems and Cubiq. Epidemiologists analyze this data and then inform state and local governments about whether social distancing orders are effective.[12] The tech companies provide aggregated data sets to the researchers, who give daily situation reports to departments of health. The researchers have justified this model based on users of the private companies' apps having consented to the collection and sharing of data.[13] I will discuss consent in more detail in a few minutes. A recent article noted that Facebook is currently sharing aggregated, anonymized location data with more than 150 organizations that are using the data for research. [14]

Governments abroad are also using technology to monitor their citizens. Last week, for example, Germany announced that its government would work with Apple and Google on its contact-tracing app, after previously supporting a home-grown alternate. In making the switch,

---

[11] *See, e.g.*, Ashkan Soltani, et al., *Contact-tracing apps are not a solution to the COVID-19 crisis*, BROOKINGS INSTITUTE (Apr. 27, 2020) ((noting also that such apps could be over or under-inclusive of potential risks and could be used maliciously), available at: https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

[12] https://www.covid19mobility.org.

[13] Caroline O. Buckee et al. "Aggregated mobility data could help fight COVID-19," 368 SCIENCE 145 (Apr. 10, 2020) (explaining that "[c]onsent-based data sharing models and data protection laws provide for the legal grounds to use personal data during emergencies"), available at: https://science.sciencemag.org/content/368/6487/145.2/tab-article-info.

[14] Kurt Wagner, *Facebook Expands Location Data Sharing with Covid-19 Researchers*, BLOOMBERG NEWS (Apr. 6, 2020), https://www.bloomberg.com/news/articles/2020-04-06/facebook-expands-location-data-sharing-with-covid-19-researchers. Facebook also has partnered with Carnegie Mellon University to distribute a symptom survey to users in the U.S., and with the University of Maryland to expand the survey globally, adding to the sensitive data Facebook will collect and share. *Id.*

Germany officials stated that the "use of a de-centralised architecture that will only store data on devices . . . is good for trust."[15]

In contrast, other countries have employed more rigorous tracking. The World Health Organization touted the stark measures taken by China as "the only measures that are currently proven to interrupt or minimize transmission chains in humans."[16] Among these measures are the "rigorous tracking and quarantine of close contacts," as well as "the use of big data and artificial intelligence (AI) to strengthen contact tracing and the management of priority populations." An ambassador for China has said his government "optimized the protocol of case discovery and management in multiple ways like backtracking the cell phone positioning."[17]

Hong Kong used "smart wristbands" initially developed to track the movements of prisoners to monitor people quarantined inside their homes.[18] The wristbands send information to the quarantined individuals' smartphones and alert the public health and law enforcement authorities if people leave their homes, break their wristbands, or disconnect them from their smartphones.[19] When first announced in early February,[20] the wristbands were required only for people who had been to Wuhan in the past 14 days, but the program rapidly expanded to encompass every person

---

[15] Douglas Busvine, *Germany flips on smartphone contact tracing, backs Apple and Google*, REUTERS (Apr. 26, 2020), https://news.trust.org/item/20200426070622-y65rz.

[16] Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19), 16-24 (Feb. 2020), available at https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-covid-19-final-report.pdf. The Chinese government has published protocols on how to handle people who came within three feet of a person confirmed or suspected to be infected with Covid-19, authorizing local law enforcement to take such close contacts into mandatory isolation if they do not voluntarily submit to medical observation – even if they test negative for the virus. See, e.g., NCP: Close Contact Management Protocol, available at https://www.fmprc.gov.cn/mfa_eng/topics_665678/kjgzbdfyyq/CERC/P020200318835652710717.pdf.

[17] H.E. Huang Zheng, *Keep calm and work shoulder to shoulder to fight the 2019-nCoV*, KASELEHLIE PRESS (Feb. 11, 2020), https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbd_665378/t1743154.shtml.

[18] Press Release: Commissioner of Correctional Services reviews CSD's work in 2018 (Feb. 14, 2020), https://www.csd.gov.hk/english/news/news_pr/20190214_1.html.

[19] Hong Kong Government: 5 contravene quarantine order (Mar. 22, 2020) https://www.news.gov.hk/eng/2020/03/20200322/20200322_223922_886.html (in addition to being sent to quarantine centers, people who contravene home quarantine are subject to criminal prosecution, a maximum fine of $25,000 and imprisonment for six months).

[20] Hong Kong Government: Smart device for home quarantine (Feb. 3, 2020), https://www.news.gov.hk/eng/2020/02/20200203/20200203_150504_450.html.

entering Hong Kong.[21] The government denied any privacy concerns about the electronic wristbands, saying the Privacy Commissioner for Personal Data had been consulted about the technology and agreed it could be used to ensure that quarantined individuals remain at home.[22]

Taiwan is using mobile device location data as an "electric fence" to monitor citizens' movements. The government obtains the SIM card identifiers for the mobile devices of quarantined individuals and passes those identifiers to mobile network operators, which use phone signals to their cell towers to alert public health and law enforcement agencies when the phone of a quarantined individual leaves a certain geographic range.[23] In response to privacy concerns, the National Communications Commission said the system was authorized by special laws to prevent the coronavirus, and that it "does not violate personal data or privacy protection."[24]

In Singapore, travelers and others were issued Stay-Home Notices that directed them to remain in their homes. When contacted by authorities, quarantined individuals must respond within an hour by phone, text message or WhatsApp.[25] And to assist with contact tracing, the government has encouraged everyone in the country to download TraceTogether, an app that

[21] Hong Kong Government: Gov't explains wristband activation, (Mar. 25, 2020), https://www.news.gov.hk/eng/2020/03/20200325/20200325_175807_517.html (the rollout initially was impeded by new arrivals sometimes not providing a phone number that could receive a text message from the government to activate the StayHomeSafe mobile app).
[22] Hong Kong Government: Wristbands pose no privacy issue, (Mar. 18, 2020), https://www.news.gov.hk/eng/2020/03/20200318/20200318_232832_530.html.
[23] Press Release: High-tech intelligent epidemic prevention, accurate and powerful quarantine tracking, Taiwan Centers of Disease Control (Mar. 18, 2020), https://www.cdc.gov.tw/Bulletin/Detail/LxV1VKIb689M9Sb1q8XOcQ?typeid=9.
[24] Press Release, "NCC clarified: Taiwan's 'Electronic Anti-epidemic Service Platform' was developed independently," National Communications Commission (Mar. 24, 2020), https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&cate=0&keyword=&is_history=0&pages=0&sn_f=42899.
[25] Government of Singapore, Everything you need to know about Stay-Home Notice (Mar. 19, 2020), https://www.gov.sg/article/everything-you-need-to-know-about-the-stay-home-notice (failure to comply may result in prosecution and up to $20,000 in a fine and a year in prison, as well as revocation of work, student and long-term visitor visas for non-citizens).

uses BlueTooth to identify other nearby phones with the app and tracks when phones are in close proximity.[26]

Poland is requiring quarantined individuals to download the "Home Quarantine" smartphone app.[27] Those who do not install and use the app are subject to a fine. The app verifies users' compliance with quarantine through selfies and GPS data. Users' personal data will be administered by the Minister of Digitization, who has appointed a data protection officer. Each user's identification, name, telephone number, quarantine location and quarantine end date can be shared with police and other government agencies. After two weeks, if the user does not report symptoms of Covid-19, the account will be deactivated – but the data will be stored for six years.[28]

In the United Kingdom, the National Health Service (NHS) is compiling online and call center data, and Covid-19 test results.[29] The NHS is working with several companies including Microsoft, Palantir Technologies, Amazon Web Services and Google, all previous targets of criticism for their privacy practices. The NHS has promised to keep the data under its control,

---

[26] Government of Singapore: Help speed up contact tracing with TraceTogether (Mar. 21, 2020) ("What about my privacy? The app does not track your location or contacts. Data is stored in your phone for only 21 days and will not be accessed unless you are identified as a close contact. Measures are in place to protect your mobile number. Your number is paired with a random ID, and it is this ID that is exchanged between phones, not your actual number."), https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether

[27] Republic of Poland: "Home Quarantine application" (Mar. 19, 2020), available at https://www.gov.pl/web/koronawirus/kwarantanna-domowa. Only people who are visually impaired, do not own a mobile device or do not subscribe to a telecommunications network are exempt from downloading the app once placed under quarantine.

[28] Poland's Ministry of Digitization has claimed that it must store the data for six years in case users pursue claims against the government. *Id.* ("The Minister stores personal data for the limitation period for claims referred to in Article 118 of the Civil Code Act (6 years).") However, local privacy expert and Panoptykon Foundation cofounder Katarzyna Szymielewicz has questioned this rationale. Szostak, Piotr "Google i Uber powinny dzielić się wiedzą o przepływach użytkowników. Nie tylko w czasie pandemii koronawirusa," Wyborcza.pl, (Mar. 26, 2020), https://wyborcza.pl/7,156282,25820437,dobrowolna-aplikacja-kwarantanna-domowa-jak-dziala-i-jak.html ("Taking all this into account, I see no reason to keep the application reports longer.")

[29] Matthew Gould, et al., *The power of data in a pandemic*, TECHNOLOGY IN THE NHS BLOG (Mar. 28, 2020) ("When the pandemic abates and the outbreak is contained, we will close the Covid-19 datastore. The Data Processing agreements put in place with the organisations listed above include the steps which need to be taken to cease processing and to either destroy or return data to NHS England and NHS Improvement once the public health emergency situation has ended."), https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/

and to require those partners to destroy or return the data "once the public health emergency situation has ended."[30] The NHS also has committed to meet the requirements of data protection legislation by ensuring that individuals cannot be re-identified from the data in the database.

Israel's Ministry of Health launched an app for mobile devices called HaMagen (the shield) to prevent the spread of coronavirus by identifying contacts between diagnosed patients and people who came into contact with them in the 14 days prior to diagnosis.[31] In March, the prime minister's cabinet bypassed the legislative body to approve emergency regulations for obtaining without a warrant the cellphone location data and additional personal information of those diagnosed with or suspected of coronavirus infection.[32] The government sent text messages to people who came into contact with potentially infected individuals, and monitored their compliance with quarantine. The Ministry of Health stated it would not hold this information; instead, it could make data requests to the police and Shin Bet, the Israel Security Agency. The police enforced quarantine measures and Shin Bet tracked down those who came into contact with potentially individuals. The Israeli parliament, however, recently suspended the use of this data, citing privacy concerns.[33]

---

[30] *Id.*

[31] The Israel Ministry of Health website states that it endorses HAMAGEN, an App to Prevent the Spread of Coronavirus: "The app can tell [if] you have been in the presence of anyone who has been diagnosed with coronavirus. The app cross-checks the GPS history of your mobile phone with historical geographic data from patients from the Ministry of Health." https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/

[32] *See, e.g.*, Noa Landau, *Israeli Coronavirus Surveillance Explained: Who's Tracking You and What Happens With the Data* HAARETZ (March 18, 2020), https://www.haaretz.com/israel-news/.premium-israeli-coronavirus-surveillance-who-s-tracking-you-and-what-happens-with-the-data-1.8685383. The Parliament later established oversight of Shin Bet's participation in the program. Knesset News: Subcommittee on Intelligence approves government's decision to allow Shin Bet to join national campaign to curb spread of coronavirus (Apr. 1, 2020) available at: https://main.knesset.gov.il/EN/News/PressReleases/Pages/press1420f.aspx.

[33] Dan Williams et al., *Israel suspends cellphone-tracking for coronavirus quarantine enforcement*, REUTERS (Apr. 22, 2020), https://www.reuters.com/article/us-health-coronavirus-israel-police/israel-suspends-cellphone-tracking-for-coronavirus-quarantine-enforcement-idUSKCN2242JJ

III. Privacy Risks from Partnerships

This quick inventory of tech-driven initiatives in several different countries reminds me of the protagonist, Phileas Fogg, in the classic tale titled *Around the World in 80 Days.* If you've ever had the pleasure of reading this book, you'll recall that Mr. Fogg wagers he can circumnavigate the globe in 80 days – no small feat before the invention of the jet engine. As he and his valet travel through different countries, they overcome kidnapping, save a damsel in distress, get mistaken for bank robbers, and incite a mutiny at sea. In other words, theirs is not a seamless trip.

As someone who cares deeply about consumer privacy, I find the tale of Mr. Fogg's trip around the world to be an apt analogy. The road to containing the virus and recovering some semblance of normal life is fraught with danger for consumer privacy and even liberty. The types of danger will differ across jurisdictions, depending on the chosen tech solution and its unique approach to data collection and use. But the danger is real, and will accompany us each step of the journey.

Let me be clear: it is understandable that for a short time, health and safety issues may take precedence over some privacy protections. And I recognize the potential for these tech-driven solutions to help mitigate the spread of the disease. But privacy cannot be an afterthought. Covid-19 presents new and complex choices about information collection, dissemination, and use. Great care is required as we navigate these choices, because privacy and data security missteps can cause irrevocable harm.

I'd like to highlight several concerns that are top of mind for me.

First, choice. We take for granted our ability to choose whether to be on social media, and whether to have our store purchases tracked over time in exchange for discounts. Now, though,

the pandemic has made some technological intrusions effectively impossible to refuse. For example, if you test positive for Covid-19, this information will be given to public health authorities. Laws, pre-pandemic, specifically allow for the sharing of this information.

In addition, with public schools and universities across the U.S. and around the world closed for the rest of the semester, students are learning online. They must consent to video classes, which entails downloading software to access classes and exams. Many students are required to have their laptop cameras and microphones active during online class sessions to verify attendance and participation. Even more are required to take exams in the presence of an online proctor who monitors for cheating via webcam.[34] (I have three college students sheltering in place with me, and more often than not, my living room and kitchen are on display for at least one professor. I can only hope our housekeeping is sufficient to avoid the professors' disdain!)

Second, the repurposing of data. Private companies have been hoovering up personal data for years. What this pandemic lays bare, though, is that while this trove of information was ostensibly collected to catalogue your coffee preferences and transportation habits, it can be repurposed in a heartbeat to restrict your movements,[35] impinge on your freedom of association,[36] and silence your freedom of speech.[37] In many instances consumers technically consented to the

[34] ProctorU Case Studies: From Florida to Nebraska, One Admin's Online Proctoring Experience Across Multiple Universities, (July 11, 2018) (school administrator describing experience at the University of Florida where a student traveling for an internship needed to be able to take exams remotely), available at: https://www.proctoru.com/industry-news-and-notes/from-florida-to-nebraska-one-admins-online-proctoring-experience-across-multiple-universities; *see also* College Board AP Testing Guide (April 2020), available at: https://apcentral.collegeboard.org/pdf/ap-testing-guide-2020.pdf?SFMC_cid=EM305179-&rid=33645968 (requiring students to use specific technology to take AP exams and agree to digital software to monitor compliance with exam regulations).

[35] James Shotter, *Slovakia to track coronavirus victims through telecoms data. Parliament passes law as Europe weighs right to privacy against moves to contain outbreak*, FINANCIAL TIMES (Mar. 25, 2020), https://www.ft.com/content/64539a44-6e87-11ea-89df-41bea055720b

[36] Andrew Crocker, et al., *The Challenge of Proximity Apps for COVID-19 Contact Tracing*, EFF (Apr. 10, 2020), https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

[37] News Release: Public Safety Director Ambrose warns against false reporting of coronavirus on social media, Newark Department of Public Safety (Mar. 10, 2020), available at: https://nextdoor.com/agency-

collection of this data – but now, the data will be used and shared in ways consumers never imagined. No one assumed a pandemic when agreeing to a company's privacy policy. In any event, the assumption that consumers have given informed consent to the collection of their data – particularly for the purpose of monitoring their compliance with social isolation measures during a pandemic – is flawed. Studies show the average consumer does not understand all the different types of data that are collected and how that information is monetized, analyzed, and shared with third parties.[38] Click-through consent does not end the conversation about privacy.

Third, the nature of the data at issue. The privacy and data security practices of healthcare and software companies will impact billions of people during and after this pandemic. The U.S. already has laws that are relevant to these areas, including the Health Insurance Portability and Accountability Act, which sets national standards for the protection of individually identifiable health information by health plans, health care providers, and others.

But technological developments have created gaps in HIPAA enforcement.[39] Sensitive medical information is now commonly stored in places other than health care practitioners'

---

post/nj/newark/newark-police-department/public-safety-director-ambrose-warns-against-false-reporting-of-coronavirus-in-newark-via-social-media-139923492/.

[38] For example, a 2014 study conducted by Pew Research found that a majority of Americans (incorrectly) believe that when a company posts a privacy policy, it ensures that the company will not share user data. Aaron Smith, *What Internet Users Know about Technology and the Web*, PEW RESEARCH CTR. (Nov. 25, 2014), https://www.pewresearch.org/internet/2014/11/25/web-iq/. Similarly, a 2015 study conducted by researchers at the University of Pennsylvania's Annenberg School of Communication found that 58% of respondents incorrectly believed and 7% responded "don't know" to the prompt: "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission." JOSEPH TUROW ET AL., U. PA. ANNENBERG SCH. FOR COMM., THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 16 (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf; *see also*, Ginger Zhe Jin & Andrew Stivers, *Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics* 6 (2017), https://ssrn.com/abstract=3006172 (arguing that a consumer is dependent on the representations made by companies or their vendors because he or she is not in a position to review and assess the privacy policies and actual practices of each company in the opaque networks of entities supporting the consumer's digital interactions); *see also* Christine S. Wilson, "A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation," Remarks at the Future of Privacy Forum, Washington, DC, February 6, 2020, n. 8-24.

[39] For example, HIPAA applies to certain doctors' offices, hospitals, and insurance companies, but not generally to cash practices, wearables, apps, or websites like WebMD. The Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d.

offices. Phones and watches now collect information about blood sugar levels, exercise habits, fertility, and heart health. Several U.S. Senators have expressed concern that the access to consumers' health data for contact-tracing could enable tech companies to build profiles of people's ailments, exposing them to potential discrimination by employers, insurance companies, landlords, or others.[40]

Fourth, the threat of constant surveillance. Employers are racing to deploy apps and technologies that will enable them to bring employees back to work safely.[41] One 32-story office building in Manhattan will use thermal cameras to measure body temperatures as employees file into the building, and plans to develop a mobile app for tenants to score workers' compliance with social distancing.[42] Another company said it is building a phone app for employers that traces contacts by analyzing workers' interactions in the office; some of the nation's biggest banks, manufacturers, and energy companies have expressed interest in using this app.[43] In India, the government announced that use of its contract-tracing app, Aarogya Setu, would be mandatory for office workers.[44]

Monitoring and tracking employees throughout the day presents obvious concerns – personally, I'm not sure my employer *really* needs to know where I get my over-priced caffeine infusion each afternoon. More fundamentally, flaws in this technology, substantively (through false positive or false negatives) or procedurally (through leaks or breaches) could expose

---

[40] Evan Halper, *Lawmarkers warn coronavirus contact tracing is ripe for abusive surveillance*, LOS ANGELES TIMES (Apr. 26, 2020), https://www.latimes.com/politics/story/2020-04-26/privacy-americans-trade-off-trace-coronavirus-contacts.

[41] *Private sector races to build virus apps to track employees*, SECURITY SURVEILLANCE (Apr. 2020), available at: https://securitydiscounts.com/2020/04/private-sector-races-to-build-virus-apps-to-track-employees/

[42] Konrad Putzier, et al., *Welcome Back to the Office. Your Every Move Will Be Watched*, WALL STREET JOURNAL (May 5, 2020), https://www.wsj.com/articles/lockdown-reopen-office-coronavirus-privacy-11588689725?mod=searchresults&page=1&pos=1.

[43] *Id.*

[44] *Coronavirus lockdown: No more voluntary, Aarogya Setu app now mandatory for office workers*, INDIA TODAY (May 1, 2020), https://www.indiatoday.in/amp/technology/news/story/coronavirus-lockdown-no-more-voluntary-aarogya-setu-app-now-mandatory-for-office-workers-1673438-2020-05-01?__twitter_impression=true.

employees to various risks and lead to abuse or misinformation.[45] Independent researchers warned that India's tracing app could leak patient locations, allowing hackers to pinpoint users who report positive diagnoses.[46]

Technology companies and public health authorities seek to assuage concerns by promising the use of aggregated and deidentified data. Undoubtedly, analysis of aggregated data will enable health authorities to see trends, and evaluate the effectiveness of stay-at-home orders, and treatments. Sharing data across jurisdictions may aid in these efforts. An International Association of Privacy Professionals (IAPP) article notes, however, that aggregated data can give a false sense of security – "the more statistics produced from the same underlying data, the more likely it is that the underlying data can be reconstructed from those statistics. This is because there are only so many combinations of data that could have produced those statistics."[47] IAPP notes that while deidentification or anonymization can control for some of these risks – removing the association between the data and people – applying these techniques to the data after the fact is less effective than applying them to the record-level data.

Fifth, evisceration of the Fourth Amendment. The Fourth Amendment protects American citizens from government action. The "reasonable expectation of privacy" test applied in Fourth Amendment cases connects the arenas of government action and commercial data collection. As Professor Paul Ohm of the Georgetown University Law Center notes, "the dramatic expansion of

---

[45] *See* Ashkan Soltani, et al., *Contact-tracing apps are not a solution to the COVID-19 crisis*, BROOKINGS INSTITUTE (Apr. 27, 2020) (noting also that such apps could be over or under-inclusive of potential risks and could be used maliciously), available at: https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

[46] Andy Greenberg, *India's Covid-19 Contract Tracing App Could Leak Patient Locations*,WIRED (May 6, 2020), https://www.wired.com/story/india-covid-19-contract-tracing-app-patient-location-privacy/?utm_source=govdelivery; *see also* Ashkan Soltani, et al., *Contact-tracing apps are not a solution to the COVID-19 crisis*, BROOKINGS INSTITUTE (Apr. 27, 2020) (warning that the apps "will serve as vehicles for abuse and disinformation"), available at: https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

[47] Luk Arbuckle, *Aggregated data provides a false sense of security*, IAPP (Apr. 27, 2020), https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/

technologically-fueled corporate surveillance of our private lives automatically expands police surveillance too, thanks to the way the Supreme Court has construed the reasonable expectation of privacy test and the third-party doctrine."[48] In other words, if citizens know and accept that nothing is private, then they have no reasonable expectation of privacy – and the Fourth Amendment gets eviscerated.

Police have long been able to enforce based on direct observation of violations. But if law enforcement authorities identify law violators – say, the contravention of stay-at-home orders – based on data collection rather than direct observation, the Fourth Amendment may be implicated. In two recent cases, *Jones* and *Carpenter*, the U.S. Supreme Court has limited the warrantless tracking of Americans through GPS devices placed on their cars and through cellphone data.[49] This same data, though, also could be used to piece together evidence of violations of stay-at-home orders. As Chief Justice John Roberts wrote in *Carpenter*, "With access to [cell-site location information], the government can now travel back in time to retrace a person's whereabouts . . . Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years."[50]

Countries globally are grappling with these privacy risks. As I noted earlier, the Israeli parliament recently suspended the use of cellphone tracking data to enforce quarantine orders. A member of the Knesset Foreign Affairs Committee noted that "[t]he utility offered by this

[48] Paul Ohm, The Many Revolutions of *Carpenter*, 32 HARV. J. L. & TECH. 357, 362 (2019). Ohm argues that the "reasonable expectation of privacy" test should be replaced by the rules outlined in *Carpenter*, allowing courts to respond "flexibly and rapidly to the insistent challenges of new technology on privacy."
[49] *United States v. Jones*, 565 U.S. 400 (2012) (overturning district court ruling that Jones had no reasonable expectation of privacy when the vehicle was on public streets, and holding that the government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment); *Carpenter v. United States*, 135 S.Ct. 2206 (2018) (5-4 ruling reversing the lower courts' view that cell-site data is comparable to mailing addresses and phone numbers, and holding that the government must obtain a warrant to access historical cellphone records; "seismic shifts in digital technology [] made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. … There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today").
[50] *Carpenter v. United States*, 135 S. Ct. 2206, 2218 (2018).

(cellphone tracking) is outweighed by the great harm inflicted to privacy."[51] Other officials, however, were pleased with the results. Proponents observed that involving the Shin Bet in tracking movements assisted in identifying new cases and that the infringements on privacy were minimal, as the relevant information is expunged after a week.[52]

As the UK embraces technology for contact tracing that requires mass adoption by consumers to be effective, UK's Information Commissioner, Elizabeth Denham, published a thoughtful piece detailing important policy considerations.[53] Commissioner Denham noted the parallels between the adoption of tech-driven Covid-19 initiatives and passage of the data protection law in the UK. The UK law "emerged out of a concern that the benefits of new technology could be lost if advances were not embraced by the population. Data protection law was seen as a way to support innovation by assuring people that checks were in place to prevent the build-up of intrusive pictures of their lives."[54] Similarly, the public must have confidence that any coronavirus technology "is being used in a fair and proportionate way."[55]

IV. Recommendations to Mitigate Risks

Privacy can coexist with a public health response fueled by big data. Unfortunately, though, the lack of federal privacy legislation in the U.S. has led to suboptimal outcomes in certain aspects of our pandemic response. Legislation would have provided clarity for businesses on the legitimate uses of data during this pandemic and established guardrails to protect against risks to privacy and civil liberties.

---

[51] Dan Williams, *Israel suspends cellphone-tracking for coronavirus quarantine enforcement*, REUTERS (Apr. 22, 2020), https://www.reuters.com/article/us-health-coronavirus-israel-police/israel-suspends-cellphone-tracking-for-coronavirus-quarantine-enforcement-idUSKCN2242JJ
[52] *Id.*
[53] Elizabeth Denham, *Combatting COVID-19 through data – some considerations for privacy*, INFORMATION COMMISSIONER BLOG POST (Apr. 17, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy/.
[54] *Id.*
[55] *Id.*

There has long been a call for federal privacy legislation. The FTC, on a bipartisan basis, recommended that Congress pass comprehensive federal privacy legislation in its first major report on privacy in 2012.[56] A confluence of events in 2018 renewed the push – passage and implementation of the Global Data Protection Regulation (GDPR) in Europe, the Cambridge Analytica revelations, and passage of the California Consumer Privacy Act (CCPA). Since joining the FTC as a Commissioner, I have echoed this long-standing call – in testimony before the U.S. Senate and House, in public speeches, and in articles.[57] The call for legislation is bipartisan, and is supported by essentially all stakeholders. And we have seen progress – notable draft and discussion draft bills recently have been circulated.[58] Regrettably, Congress has failed to enact privacy legislation.

In the absence of comprehensive federal privacy legislation, the FTC has built an impressive record of protecting consumers' privacy and data security using its general consumer protection

---

[56] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. The Report stated: "The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates it call for data security legislation." In the absence of legislation, the Commission urged "industry to accelerate the pace of self-regulation." *Id.* at i.

[57] *See* Christine Wilson, *Privacy in the Time of Covid-19*, TRUTH ON THE MARKET (Apr. 15, 2020), https://truthonthemarket.com/author/christinewilsonicle/; Christine S. Wilson, "A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation," Remarks at the Future of Privacy Forum, Washington, DC, February 6, 2020, https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf; Oral Statement of Commissioner Christine S. Wilson Before the U.S. House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce (May 8, 2019), https://www.ftc.gov/system/files/documents/public_statements/1519254/commissioner_wilson_may_2019_ec_opening.pdf; Oral Statement of Commissioner Christine S. Wilson, FTC, Before the U.S. Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security (Nov. 27, 2018), https://www.ftc.gov/system/files/documents/public_statements/1423979/commissioner_wilson_nov_2018_testimony.pdf.

[58] Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 108 (as introduced in the Senate by Senator Cantwell, December 3, 2019), https://www.congress.gov/116/bills/s2968/BILLS-116s2968is.pdf; Senator Wicker, Discussion Draft, United States Consumer Data Privacy Act of 2019, § 201, https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf; *see also* H. Energy & Commerce Comm., Discussion Draft, Bipartisan Data Privacy Bill, 23-25, https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/2019.12.18-Privacy-Bipartsian-Staff-Discussion-Draft.pdf.

authority and its authority under narrow privacy statutes. Professor Solove himself has written about the common law of privacy the FTC has created.[59] But there are significant limits to our authority.[60] The FTC recently confronted these limits in its enforcement action against Facebook,[61] a reality the district court acknowledged in its opinion when it entered the Facebook order last week. Specifically, the judge wrote that some of the allegations against Facebook "call into question the adequacy of laws governing how technology companies that collect and monetize Americans' personal information must treat that information." He also agreed with the FTC that this is a Congressional issue.[62]

A group of Republican Senators recently introduced a bill, the "COVID-19 Consumer Data Protection Act," to address some of the privacy risks of this pandemic.[63] This is a welcome development but I believe comprehensive legislation is preferable to a short-term solution that addresses issues only in the context of the current crisis. Legislation could promote responsible and transparent uses and allow for disclosures for public health. Analogues appear in existing statutes. HIPAA, for example, includes provisions that permit the release of private health data

---

[59] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 COLUMBIA L. REV. 583 (2014). Solove and Woodrow explain that FTC settlements have created a common law of privacy. "[C]ompanies look to these agreements to guide their privacy practices. Thus, in practice FTC privacy jurisprudence has become the broadest most influential regulating force on information privacy in the United States – more so than nearly any privacy statute or any common law tort." *Id.*

[60] For example, the FTC does not have authority under Section 5 to impose penalities on entities for first time privacy or security violations, does not have jurisdiction over non-profits or common carriers – although these entities collect and process significant amounts of consumer data – and does not have general notice and comment rulemaking authority to promulgate rules to address privacy and data security practices.

[61] Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson, In re Facebook (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf; Prepared Remarks of Commissioner Christine S. Wilson, Facebook., Inc. Press Event (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1537163/wilson_-_prepared_remarks_at_ftc_facebook_press_conference_7-24-19_0.pdf; Christine S. Wilson, Remarks at the Global Antitrust Institute: FTC vs. Facebook, Antonin Scalia Law School 6, 10 (Dec. 11, 2019), https://www.ftc.gov/system/files/documents/public_statements/1557534/commissioner_wilson_remarks_at_global_antitrust_institute_12112019.pdf.

[62] U.S. v. Facebook, Inc., No. 19-2184 (TJK) at 1-2 (D.D.C. Apr. 23, 2020); available at: https://www.courtlistener.com/pdf/2020/04/23/united_states_v._facebook_inc._1.pdf.

[63] The COVID-19 Consumer Data Protection Act, available at: https://www.commerce.senate.gov/2020/4/wicker-thune-moran-blackburn-announce-plans-to-introduce-data-privacy-bill

by covered entities/individuals for public health activities.[64] Similarly, the Children's Online Privacy Protection Act specifically permits the collection of personal information from a child, without parental consent, to protect the safety of the child.[65]

Even absent legislative limits, companies and governments should seek to mitigate risks and earn consumer trust. Building digital trust is always important. But when the efficacy of a voluntary contact-tracing app depends on convincing a critical mass of citizens to opt in, the incentives to build trust are greater. A recent Washington Post/University of Maryland poll found that 60% of Americans are not willing or able to use the contract-tracing app that Apple and Google are developing.[66] If public health authorities are going to rely on these apps, then researchers, companies, and governments need to bridge the trust gap. Responsible companies will reap the benefits of these actions in the post-pandemic commercial world.

Beginning with its seminal 2012 privacy report, the FTC has urged technology companies "to implement best practices to protect consumers' private information," to make privacy the "default setting," and to use privacy by design – "[b]uild privacy at every stage of product development."[67] The FTC website offers many easily accessible resources that explain how to do this, including Protecting Personal Information: A Guide for Business,[68] Start with Security:

---

[64] The Health Insurance Portability and Accountability Act of 1996, 45 CFR 164.512(b) (providing for public health authorities to receive health information for the purpose of preventing or controlling disease).
[65] Children's Online Privacy Protection Rule, 16 CFR 312.5(c)(5) (providing an exception to the requirement to obtain parental consent "[w]here the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety.")
[66] Craig Timberg, *Most Americans Are Not Willing or Able to Use an App Tracking Cornavirus Infections*, WASHINGTON POST (Apr. 29, 2020), https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/
[67] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE at i (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
[68] FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESSES (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

A Guide for Business,[69] and Stick with Security: A Business Blog Series.[70] While the Gramm-Leach-Bliley Act (GLB) only applies to financial institutions, the FTC's GLB compliance blog outlines a number of data security best practices.[71] In addition, the FTC's privacy and data security orders lay out the key elements of privacy and data security programs.[72] And, in the last few weeks, FTC staff have compiled several excellent guidance documents for consumers and businesses relevant to consumer privacy and data security in these uncertain times, including COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus;[73] Using Artificial Intelligence and Algorithms;[74] and Video Conferencing: 10 privacy tips for your business.[75]

There are comprehensive resources outside the FTC as well. The National Institute for Standards and Technology (NIST) offers a number of security and privacy materials, including a

---

[69] FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESSES (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *see also* FED. TRADE COMM'N, APP DEVELOPERS: START WITH SECURITY (2017), https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security (detailing security practices for app developers).

[70] FED. TRADE COMM'N, STICK WITH SECURITY: A BUSINESS BLOG SERIES (2017); https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series

[71] FED. TRADE COMM'N, FINANCIAL INSTITUTIONS AND CUSTOMER INFORMATION: COMPLYING WITH THE SAFEGUARDS RULE (2006); https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

[72] *See, e.g.*, In the Matter of Facebook, Inc. C-4365 (2020) (modified administrative order requiring a comprehensive privacy and data security program resolving prior order violations), https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf; In the Matter of LightYear Dealer Technologies, LLL C-4687 (2019) (data security order); https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf; In the Matter of Uber Technologies, Inc. C-4662 (2018) (privacy order), https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf; FTC, et al. v. Vizio, Inc., et al., No.2:17-cv-00758 (D.N.J 2017) (privacy order), https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf; *see also* Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 COLUMBIA L. REV. 583 (2014) (describing the "common law of privacy" created by FTC consents).

[73] Lisa Schifferle, *COPPA Guidance for Ed Tech Companies and Schools During the Coronavirus*, FED. TRADE COMM'N, (APR. 9, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus.

[74] Andrew Smith, *Using Artificial Intelligence and Algorithms*, FED. TRADE COMM'N (Apr. 8 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms.

[75] Jonah Fabricant, *Video conferencing: 10 privacy tips for your business*, FED. TRADE COMM'N (Apr. 16, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business.

privacy framework to help organizations identify and manage privacy risks.[76] Private organizations like the IAPP and the App Association also have published helpful resources,[77] as have trade associations. Our international counterparts offer excellent materials as well. The blog post I discussed earlier by UK Information Commissioner Elizabeth Denham includes a series of simple, yet comprehensive, questions to guide analysis and evaluation of new technologies and procedures.[78]

One privacy best practice that is particularly relevant now is accountability. The Center for Information Policy Leadership (CIPL), which operates here and internationally, has produced several white papers detailing privacy best practices that focus on accountability.[79] In particular, CIPL's July 2018 discussion paper, The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, includes an accountability wheel that provides an excellent visual framework for businesses to design privacy programs for emerging technologies assisting with combatting Covid-19.[80]

---

[76] NIST Privacy Framework, available at: https://www.nist.gov/privacy-framework

[77] IAPP's website offers articles, resources and courses on privacy, including a three part series on privacy programs, https://iapp.org/resources/article/for-a-successful-privacy-program-use-these-three-as-three-part-series/. The App Association offers a number of resources to help mobile developers think through privacy risks in the app space, https://actonline.org/resources/.

[78] The questions include: Have you demonstrated how privacy is built in to the processor technology? Is the planned collection and use of personal data necessary and proportionate? What control do users have over their data? How much data needs to be gathered and processed centrally? When in operation, what are the governance and accountability processes in your organization for ongoing monitoring and evaluation of data processing – to ensure it remains necessary and effective, and to ensure that the safeguards in place are still suitable? What happens when the processing is no longer necessary? Elizabeth Denham, *Combatting COVID-19 through data – some considerations for privacy*, INFORMATION COMMISSIONER BLOG POST (Apr. 17, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy/..

[79] CIPL offers a number of White Papers on effective elements of privacy programs, https://www.informationpolicycentre.com/cipl-white-papers.html. CIPL also recently published a Covid-19 Case Study for Accountability to assist companies with complying with privacy laws and also "create openness around decision-making processes for data use and sharing, thereby generating public trust." Covid-19 Meets Privacy: A Case Study for Accountability (April 2020), available at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/04/covid-19_meets_privacy_a_case_study_for_accountability_-_centre_for_information_policy_leadership__april_2020_.pdf

[80] CIPL: The Case of Accountability: How it Enables Effective Data Protection and Trust in the Digital Society (July 2018), available at:

The center of the wheel sets out the overarching goal – "Accountability, Effective Compliance and Protection for Individuals." The circles arrayed around the center identify seven elements of accountability: leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement. I recommend that companies evaluate their privacy programs in light of these elements, considering carefully each of these areas.

First, leadership and oversight are essential to an effective privacy program. As I have emphasized in connection with our Facebook settlement, a culture of compliance begins at the top. If the CEO views privacy protection as a priority, employees will respond in kind. Companies should designate a qualified employee or group to coordinate and be responsible for the privacy program, with oversight and active leadership of senior management, and the board where applicable.[81] When developing tech to respond to this pandemic, the team should include at least one person responsible for considering privacy and security at every stage of the program's development and implementation.

Second, risk assessments play a key role in every privacy program. Companies should assess and document, at every stage of product development and throughout the business operation, the internal and external risks to the privacy, confidentiality, integrity, and use of data that could

---

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf

[81] FTC orders requiring a comprehensive privacy program consistently include this as a requirement. *See, e.g.*, In the Matter of Facebook, Inc. C-4365 (2020) (modified administrative order requiring a comprehensive privacy and data security program resolving prior order violations), https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf; In the Matter of Uber Technologies, Inc. C-4662 (2018) (privacy order), https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf; FTC, et al. v. Vizio, Inc., et al., No.2:17-cv-00758 (D.N.J 2017) (privacy order), https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.

result in unauthorized access, collection, use, destruction, or disclosure.[82] This is particularly important as businesses rapidly develop new technology in response to Covid-19. Although time is of the essence as the coronavirus continues to spread, skipping this step is not a wise shortcut.

Third, policies and procedures – companies should design, implement, and maintain policies and procedures that control for the internal and external risks identified in the risk assessments.[83] These policies and procedures should identify the purposes for data collection, and the uses to which the data will be put. They should also address employee access, training, storage, security, and deletion. Data collection should be proportional, ensuring that companies do not collect more than needed for the intended purpose. This concept is particularly relevant to contract tracing and other monitoring technology. Companies should carefully consider the data that is truly necessary and only collect that data – for example, if names and emails are not truly needed, do not collect them.

Companies also should use privacy protective technologies, like encryption, and rely on deidentified & aggregated data as much as possible. Data should be released or shared only with those people who need it for approved purposes in data-protected enviroments.[84] And privacy

---

[82] FTC orders requiring a comprehensive privacy program typically require risk assessments. *See supra* n. 72 (privacy orders); *see also* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESSES (2016) (recommending that companies inventory the personal information collected, including what data collected and how data is stored, accessed, used and shared), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf; *see also* FED. TRADE COMM'N, APP DEVELOPERS: START WITH SECURITY (2017) (detailing privacy and security practices for app developers), https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security.

[83] *See supra* n. 72 (privacy orders); *see also* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESSES (2016) (describing best practices of policies and procedures for data collection, use, access, maintenance, and sharing), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf; FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESSES (2015) (detailing best practices for privacy and security from lessons learned in FTC enforcement actions), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *see also* FED. TRADE COMM'N, APP DEVELOPERS: START WITH SECURITY (2017) (detailing privacy and security practices for app developers), https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security.

[84] FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESSES (2016) (describing best practices of policies and procedures for data collection, use, access, maintenance, and sharing), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf; FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESSES (2015) (detailing best practices for privacy and

program policies and procedures also should include pre-established metrics for halting the collection and sharing of data, as well as the destruction and deletion of data, once this crisis abates.[85]

The use of AI technology to make predictions, recommendations or decisions holds enormous potential and is likely to be employed in combatting this pandemic.[86] It also presents risks, including the potential for unfair or discriminatory outcomes or the perpetuation of existing socioeconomic disparities.[87] Therefore, companies should ensure AI-based decisions are fair and that data models are robust and sound (validated and re-validated to make sure they do not discriminate), and hold themselves accountable for compliance, ethics, fairness, and non-discrimination.

Fourth, transparency – companies should be transparent with consumers about the collection and use of data, including new uses of previously provided data.[88] Allowing consumers to opt in is preferable but over-reliance on notice and consent should be avoided given what we know

---

security from lessons learned in FTC enforcement actions), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; FED. TRADE COMM'N, APP DEVELOPERS: START WITH SECURITY (2017) (detailing privacy and security practices for app developers), https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security; *see also* Luk Arbuckle, *Aggregated data provides a false sense of security*, IAPP (Apr. 27, 2020), https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/. IAPP recommends using simple data sets (region, sex, age) with no accompanying summary statistics produced from underlying data and for specific reporting period with no overlap from previous reporting periods. *Id; see also* Luk, Arbuckle, The Five Safes of Risk-Based Anonymization, 17 IEEE SECURITY & PRIVACY (2019), available at: https://ieeexplore.ieee.org/document/8821469

[85] FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESSES (2016) (describing best practices of policies and procedures for data hygiene and minimization), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf; FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESSES (2015) (detailing best practices for privacy and security for data hygiene and minimization), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *see also* FED. TRADE COMM'N, APP DEVELOPERS: START WITH SECURITY (2017) (detailing privacy and security practices for app developers), https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security.

[86] Andrew Smith, *Using Artificial Intelligence and Algorithms*, FED. TRADE COMM'N (Apr. 8 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms.

[87] For example, a recent study in health science revealed that an algorithm intended to target medical interventions to the sickest patients ended up funneling resources to a healthier, white population, to the detriment of sicker, black patients. *Id.*

[88] FTC privacy and data security orders provide helpful insight on transparency as these orders prohibit misrepresentations about how companies maintain the privacy, security and integrity of consumer data and require affirmative disclosures and consent for certain uses of data. *See supra* n. 72 (privacy and data security orders).

about the effectiveness (of lack thereof) of privacy disclosures in the technology space. Further, lengthy fine-print disclosures are insufficient, especially if assent is framed as an altruistic act to aid public health. Companies also should be transparent with consumers about use of AI.[89] With Covid-19 related tech, transparency is particularly essential as data is being used and shared in ways many consumers likely could not have imagined.

Fifth, training and awareness – companies must train employees on their roles and responsibilities with respect to the privacy program.[90] Policies and procedures can be implemented effectively only if they are communicated to employees and third-party vendors, and responsible parties are trained on implementation. Companies leveraging existing technology, or creating new platforms or services for Covid-19, must train their staff on the privacy and security procedures related to the technology.

Sixth, monitoring and verification – once procedures are in place, companies must monitor and verify internal and external compliance through audits and assessments, to ensure that employees and third-parties are complying with access controls, use and sharing protocols and limitations, and deletion and destruction.[91] In other words, the emphasis on privacy continues after the technology is launched. Companies need to remain involved to ensure that staff, third parties with whom they share data, and vendors are complying with procedures.[92]

---

[89] Andrew Smith, *Using Artificial Intelligence and Algorithms*, FED. TRADE COMM'N (Apr. 8 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms.

[90] *See* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESSES (2016) (providing detailed recommendations for training and communication to employees and vendors), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[91] FTC privacy and security orders require assessments, including by independent third-parties, to monitor compliance. *See supra* n. 72 (privacy and data security orders); *see also* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESSES (2015) (detailing best practices to monitor and assess procedures and employee and vendor compliance with procedures), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[92] *See* FED. TRADE COMM'N, APP DEVELOPERS: START WITH SECURITY (2017) (detailing privacy and security practices for app developers), https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security.

Finally, seventh, response and enforcement – responsible companies must establish appropriate procedures to respond to complaints and inquiries and address any non-compliance. Given the time pressure, it is inevitable that mistakes will be made and risks will be exposed as tech is pushed out for this pandemic. Companies must be responsive to developments and enforce non-compliance.

Most of these best practices apply to governments and researchers as well as private actors. Given the proliferation of public/private partnerships, federal, state, and local authorities as well as well as academics should be intentional about accountability. The practices employed now will have long-term implications – all entities involved should take care to ensure that the precedents are constructive.

V. Conclusion

As I close, allow me to offer another understatement – we are living in a unique time. As we shelter at home, technology has enabled us to stay connected to our jobs, to loved ones, to news and entertainment, and to learning opportunities like this conference. And as societies seek to reopen economies and community interactions, Big Tech is almost certainly going to be part of the solution. My goal today is to encourage all stakeholders to weave privacy systematically into the solution. With appropriate guardrails, we can ensure that government and its private partners maintain appropriate boundaries while addressing this public health crisis.