***American University Law Review* Annual Symposium Panel Discussion**
"Contact Tracing and Other Innovative Technological Responses"
Thursday, February 4, 2021, 6:30–7:30 p.m.
Background Educational Materials: Continuing Legal Education

Executive Summary

On Thursday, February 4, 2021 from 6:30–7:30 p.m. Eastern Time, the American University Law Review *will host a panel discussion on the legal questions posed by contact tracing and other innovative technological options developed in response to the COVID-19 pandemic. Panelists discussing this fascinating topic include* ***Greg Nojeim****, Senior Counsel and Director of the Freedom, Security, and Technology Project at the Center for Democracy & Technology;* ***Professor Matt Perault****, Professor at* Duke University*'s* Sanford School of Public Policy *and Director of the* Duke *Center on Science & Technology Policy; and* ***Dr. Anne L. Washington****, Assistant Professor of Data Policy at the* Steinhardt School of Culture, Education, and Human Development *at* New York University. ***Professor Jennifer Daskal****, Professor of Law and Faculty Director of the Tech, Law & Security Program at the* American University Washington College of Law*, will moderate this discussion.*

Background

In late 2019, a novel coronavirus that causes a disease known as COVID-19 began to spread rapidly through mainland China, garnering international attention as clusters formed and spread internationally at the turn of the year.[1] Given the virus's uniquely high infection rate[2] and some infected individuals' asymptomatic presentation,[3] public health authorities around the world struggled in critical early days to control the virus's spread—particularly in the United States, where the federal government quickly delegated the brunt of pandemic management to state public

1. *See* Michelle L. Holshue et al., *First Case of 2019 Novel Coronavirus in the United States*, 382 NEW ENG. J. MED. 929, 929 (2020) (detailing the first documented case of COVID-19 in the United States).

2. *See* Joe Hilton & Matt J. Keeling, *Estimation of Country-Level Basic Reproductive Ratios for Novel Coronavirus (SARS-CoV-2/COVID-19) Using Synthetic Contact Matrices*, PLOS COMPUTATIONAL BIOLOGY (July 2, 2020), https://www.medrxiv.org/content/medrxiv/early/2020/02/27/2020.02.26.20028167.full.pdf [https://perma.cc/RN7F-YLXU] (estimating COVID-19's *R* value as hovering between two and three); *see also* David Adam, *A Guide to* R*—The Pandemic's Misunderstood Metric*, NATURE (July 3, 2020), https://www.nature.com/articles/d41586-020-02009-w [https://perma.cc/PY7J-LV4D] (describing infectious diseases' reproduction number, signified in practice by the variable *R*, as the average number of people each person with a disease then infects).

3. Andreas Kronbichler et al., *Asymptomatic Patients as a Source of COVID-19 Infections: A Systematic Review and Meta-Analysis*, 98 INT'L J. INFECTIOUS DISEASES 180, 181 (2020) (reporting the results of an analysis of asymptomatic patients testing positive for the novel coronavirus).

health officials.[4] By March 11, 2020, the World Health Organization (WHO) classified COVID-19 as a pandemic,[5] and the virus's grip on society has persisted since.[6]

Following early missteps complicated by the virus's novel nature, governments around the world responded by deploying innovative technologies to track not only infection rates and hospital capacities, but also their own citizens' behavior.[7] South Korea, which international public health leaders have praised for its pandemic management, implemented an augmented contact tracing methodology using citizens' credit card transaction data, surveillance camera footage, and smartphone location data to obtain immediate information for both public health authorities and citizens,[8] building off the foundation of "manual contact tracing."[9] Seeing the success of South Korea's efforts—the nation contained the virus in the pandemic's early days despite the country's density and abstention from shelter-in-place orders[10]—other nations in the virus's grip, such as

---

4. *See* Peter Nicholas & Kathy Gilsinan, *The End of the Imperial Presidency*, THE ATL. (May 2, 2020), https://www.theatlantic.com/politics/archive/2020/05/trump-governors-coronavirus/611023 ("Trump's posture has forced governors to confront a worldwide crisis they wouldn't have imagined would be theirs to solve. They've had to venture into a chaotic global marketplace to hunt for masks and ventilators. They've forged alliances to figure out the smartest ways to reopen their economy and curb the virus's spread. And they're building systems to help them cope with future pandemics."); Farid Rahimi & Amin Talebi Bezmin Abadi, *Challenges of Managing the Asymptomatic Carriers of SARS-CoV-2*, 37 TRAVEL MED. & INFECTIOUS DISEASE 1, 1 (2020) (emphasizing the unique challenges asymptomatic patients pose to containment efforts); *see also* Darryl Fears et al., *As National Parks Remain Open During a Pandemic, Seven Workers Are Infected*, WASH. POST (Apr. 1, 2020, 7:02 PM), https://www.washingtonpost.com/climate-environment/2020/03/31/national-parks-coronavirus (detailing viral spread in national parks, which are managed by the federal Department of the Interior).

5. Tedros Adhanom Ghebreyesus, Dir.-Gen., World Health Org., Opening Remarks at the Media Briefing on COVID-19 (Mar. 11, 2020), https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020 [https://perma.cc/7VNK-EHLU].

6. *See Coronavirus World Map: Tracking the Global Outbreak*, N.Y. TIMES (Feb. 3, 2021, 7:49 AM), https://www.nytimes.com/interactive/2020/world/coronavirus-maps.html#countries [https://perma.cc/4SKG-NRLX].

7. *See* Natasha Singer & Choe Sang-Hun, *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, N.Y. TIMES (Mar. 23, 2020), https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html. *See generally* BENJAMIN BOUDREAUX ET AL., RAND CORP., DATA PRIVACY DURING PANDEMICS iii (2020), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA365-1/RAND_RRA365-1.pdf [https://perma.cc/JAX2-VGKC].

8. *See* Singer & Sang-Hun, *supra* note 7. *See generally* Brian Kim, *Lessons for America: How South Korean Authorities Used Law to Fight the Coronavirus*, LAWFARE (Mar. 16, 2020, 2:39 PM), https://www.lawfareblog.com/lessons-america-how-south-korean-authorities-used-law-fight-coronavirus [https://perma.cc/7XLZ-2PVL].

9. *See* Albert Gidari, *Manual Contact Tracing Has Privacy Issues*, CTR. FOR INTERNET & SOC'Y AT STAN. L. SCH. (May 22, 2020, 12:00 AM), http://cyberlaw.stanford.edu/blog/2020/05/manual-contact-tracing-has-privacy-issues [https://perma.cc/4MK3-XZDE] (providing a brief background to manual contact tracing and articulating numerous issues with its deployment on a broad scale in the United States); Sharon Otterman, *N.Y.C. Hired 3,000 Workers for Contact Tracing. It's Off to a Slow Start.*, N.Y. TIMES (June 21, 2020), https://www.nytimes.com/2020/06/21/nyregion/nyc-contact-tracing.html?smid=tw-share (noting that manual contact tracing retains some deficiencies that hamper its efficiency in tracking the spread of COVID-19).

10. Jake Kwon et al., *South Korea Warns of First Potential Lockdown as Coronavirus Numbers Continue to Rise*, CNN (Dec. 16, 2020, 6:16 AM), https://www.cnn.com/2020/12/16/asia/south-korea-japan-coronavirus-intl-hnk/index.html [https://perma.cc/B7M7-XXXY] (attributing South Korea's early success to its testing-

France[11] and Italy,[12] considered (and eventually implemented) similar augmented tracing approaches.[13] Likewise, Israel began tracking its citizens' movements through sophisticated analysis of "secret" cell phone data, despite previous mandates limiting use of that data to counterterrorism efforts.[14] China's virus-prompted data collection, which stemmed from a mandated contact tracing phone application (app), appeared to send users' cell phone location information directly to the police.[15]

Viewing the success of this augmented approach, the United States—which has struggled mightily since the coronavirus first arrived on its shores[16]—has expressed interest in utilizing similar data points for its own public health surveillance system, particularly among scientists on the front lines of response.[17] Though the United States has not established a federal contact tracing

---

heavy and augmented contact tracing approach); Norimitsu Onishi & Constant Mehéut, *France Weighs Its Love of Liberty in Fight Against Coronavirus*, N.Y. TIMES (Apr. 17, 2020), https://www.nytimes.com/2020/04/17/world/europe/coronavirus-france-digital-tracking.html (same).

11. *See* Onishi & Mehéut, *supra* note 10.

12. *See* Singer & Sang-Hun, *supra* note 7.

13. *See* Onishi & Mehéut, *supra* note 10; Singer & Sang-Hun, *supra* note 7.

14. David M. Halbfinger et al., *To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data*, N.Y. TIMES (Mar. 16, 2020), https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html.

15. Paul Mozur et al., *In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags*, N.Y. TIMES (Mar. 1, 2020), https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html (describing a *New York Times* analysis of Alipay Health Code, a Chinese government-mandated phone app that determines if the phone's user is a contagion risk). Notably, while Chinese technology companies often share user data with the Chinese government, the process is "rarely so direct" as Alipay Health Code. *Id.* The app's code contains an explicit direction to "reportInfoAndLocationToPolice," including the user's location and an identifying code number, as soon as the user grants the software access to the personal data on their phone. *Id.*

16. *See Coronavirus World Map: Tracking the Global Outbreak*, *supra* note 6 (detailing total COVID-19 cases and deaths, with the United States leading the world in both totals).

17. *See* Singer & Sang-Hun, *supra* note 7; Tony Romm et al., *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, WASH. POST (Mar. 17, 2020, 9:15 PM), https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus; Kirsten Grind et al., *To Track Virus, Governments Weigh Surveillance Tools that Push Privacy Limits*, WALL ST. J. (Mar. 17, 2020, 7:55 PM), https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841; Tony Romm, *White House Asks Silicon Valley for Help to Combat Coronavirus, Track Its Spread and Stop Misinformation*, WASH. POST (Mar. 11, 2020, 3:55 PM), https://www.washingtonpost.com/technology/2020/03/11/white-house-tech-meeting-coronavirus; *see also* Letter from Enid Zhou, Open Gov't Counsel, Elec. Privacy Info. Ctr., & John Davisson, Counsel, Elec. Privacy Info. Ctr., to Douglas Hibbaed, Chief, Initial Request Staff, Off. of Info. Pol'y, Dep't of Just. (Mar. 24, 2020), https://epic.org/foia/doj/covid-19/EPIC-20-03-24-DOJ-FOIA-20200324-Request.pdf [https://perma.cc/28LP-YLJW] (filing a Freedom of Information Act request with the U.S. Department of Justice regarding its interest in collecting citizens' cell phone location information). *See generally* CTRS. FOR DISEASE CONTROL & PREVENTION, PUBLIC HEALTH SURVEILLANCE: PREPARING FOR THE FUTURE (2018), https://www.cdc.gov/surveillance/pdfs/Surveillance-Series-Bookleth.pdf [https://perma.cc/8SF4-HJ4R]; KAVYA SEKAR, CONG. RSCH. SERV., IN11361, COVID-19: U.S. PUBLIC HEALTH DATA AND REPORTING (2020). Notably, as of mid-March 2020, when the United States began implementing lockdown measures, the nation's largest wireless carriers did not indicate plans to share customers' location data with the federal government. Craig Timberg & Drew Harwell, *Government Efforts to Track Virus Through Phone Location Data Complicated by Privacy Concerns*, WASH. POST (Mar. 19, 2020, 5:25 PM), https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data.

program,[18] technological tools such as facial recognition software and aggregated location data promise valuable information to public health authorities, and state departments of health leading the charge in pandemic management stand to benefit.[19] The United States is no stranger to this technology: its use has become commonplace in some federal agencies—particularly those dedicated to policing the nation's borders and ports of entry—and even in some state and local police forces.[20]

While public health authorities and medical researchers have advocated for this data collection and enhanced surveillance,[21] privacy advocates have indicated hesitation and concerns regarding unchecked government access to this technology and the data arising from it.[22] Though many of

---

18. *See* Christie Aschwanden, *Contact Tracing, a Key Way to Slow COVID-19, Is Badly Underused by the U.S.*, SCI. AM. (July 21, 2020), https://www.scientificamerican.com/article/contact-tracing-a-key-way-to-slow-covid-19-is-badly-underused-by-the-u-s [https://perma.cc/TC7T-TTGF] ("[N]o federal dollars have been specifically allocated to contact tracing 'or to any federal contact tracing programs.'").

19. Researchers have advocated for implementing these technologies to stop the virus. *See* Luca Ferretti et al., *Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing*, 368 SCIENCE 1, 1, https://science.sciencemag.org/content/sci/368/6491/eabb6936.full.pdf [https://perma.cc/3STS-DXZD]; *see also infra* notes 26–82 and accompanying text (discussing these technologies and how they benefit public health officials).

20. *See, e.g.*, Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019, 3:54 PM), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches (detailing Federal Bureau of Investigation and Immigration and Customs Enforcement officials' mining of state driver's license databases with facial recognition technology); Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS (Feb. 27, 2020, 11:37 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/YW4G-89BK]; Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html (detailing Florida police's use of facial recognition technology); Jillian D'Onfro, *This Map Shows Which Cities Are Using Facial Recognition Technology—and Which Have Banned It*, FORBES (July 18, 2019, 12:58 PM), https://www.forbes.com/sites/jilliandonfro/2019/07/18/map-of-facial-recognition-use-resistance-fight-for-the-future/?sh=23ce6c7b7e61 [https://perma.cc/XA57-3E5Y].

21. *See* Ferretti et al., *supra* note 19.

22. *See, e.g.*, Timberg & Harwell, *supra* note 17 ("'There's no reason to have to throw out our principles like privacy and consent to do this,' said Peter Eckersley, an artificial intelligence researcher who organized an open letter on ways the tech industry could help combat the outbreak."); Letter from Anna G. Eshoo, Representative, U.S. House of Representatives, Suzan K. DelBene, Representative, U.S. House of Representatives, & Ron Wyden, Senator, U.S. Senate, to Donald J. Trump, President of the United States, & Michael R. Pence, Vice President of the United States (Mar. 19, 2020), https://eshoo.house.gov/sites/eshoo.house.gov/files/documents/Eshoo-Wyden-DelBene%20-%20Letter%20to%20Pres%20%26%20VP%20about%20coronavirus%20privacy%20-%203.19.20.pdf [https://perma.cc/22VL-5374]; Mike Giglio, *Would You Sacrifice Your Privacy to Get out of Quarantine?*, THE ATL. (Apr. 22, 2020), https://www.theatlantic.com/politics/archive/2020/04/coronavirus-pandemic-privacy-civil-liberties-911/609172. Of central concern to many of these privacy advocates is the degree to which this "anonymized" data is truly anonymized. "Privacy experts repeatedly have shown that supposedly anonymous data can still be used to identify individual people, based on their known movements and other markers. Data that's both anonymous and aggregated is far more private but also less useful in identifying people at particular risk for contracting coronavirus and spreading it to others." Timberg & Harwell, *supra* note 17; *see also* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y.

these advocates acknowledge the legitimate need and unprecedented circumstances prompting these asks,[23] some have warned of possible "surveillance creep" lingering long after the pandemic's end,[24] while others have drawn parallels to the proliferation of surveillance following the September 11, 2001 terror attacks.[25]

Looming behind this debate is a complex set of legal questions rendered all the more confounding by the context under which they have arisen—namely, states of emergency on both the federal and state level (and the unique powers arising under them). This panel discussion will center on the proliferation of these technologies, the actors seeking their use, and the pertinent legal issues as the world continues to grapple with COVID-19.

Applicable Technologies

GPS Location Data. The federal government has floated the collection of citizens' cell phone location data in anonymized, aggregate form to attempt to map the spread of the coronavirus.[26] In particular, government officials seemed most interested in obtaining data that could explain patterns of people's movements and assist in identifying the newest "hotspot[s]," or, potentially, areas where medical resources are most needed.[27] Of course, a traditional contact tracing app—such as China's Alipay Health Code—could analyze a user's backlogged cell phone location information to determine if the user had been in close contact with someone who later tested positive for COVID-19; however, such a system would require a massive central repository to store the necessary data.[28] South Korea also utilized GPS location technology in its mandated COVID-19

TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

23. *See* Giglio, *supra* note 22 (relaying many such opinions from privacy experts).

24. *See, e.g.*, Robert E.G. Beens, *Privacy in a Post-Pandemic World*, FORBES (June 23, 2020, 9:10 AM), https://www.forbes.com/sites/forbestechcouncil/2020/06/23/privacy-in-a-post-pandemic-world/?sh=719c7de02b0a [https://perma.cc/AU4X-FQ65]; Giglio, *supra* note 22 ("But the erosion of privacy weakens a democracy, those such as Cohn argue, leaving people feeling as if they've lost control not just over their government, but over their personal life—and the ability to think, act, and communicate without the expectation that someone is watching or listening is fundamental to a thriving democracy."); *id.* (quoting former CIA operative and current Georgetown University professor Douglas London as saying, "I think Americans should resist such measures. Once you give away those rights and privacies, you're never going to get them back. And once the government has these powers, they can be used for other things, and they can be abused."); *id.* (quoting University of Minnesota Law School Professor Alan Rozenshtein as stating: "There really is such a thing as surveillance creep, and surveillance programs do tend to increase beyond their initial scope . . . . Pandemics, like other emergencies, have often been these catalyst moments for the permanent expansion of the government. And the government does not tend to shrink after the moment has passed."); Arjun Kharpal, *Use of Surveillance to Fight Coronavirus Raises Concerns About Government Power After Pandemic Ends*, CNBC (Mar. 26, 2020, 7:58 PM), https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html [https://perma.cc/4ZJ2-7Z28].

25. *See* Timberg & Harwell, *supra* note 17; Giglio, *supra* note 22.

26. *See* Romm et al., *supra* note 17.

27. *Id.* ("We're exploring ways that aggregated anonymized location information could help in the fight against COVID-19. One example could be helping health authorities determine the impact of social distancing, similar to the way we show popular restaurant times and traffic patterns in Google Maps . . . .").

28. *See* Kieren McCarthy, *So How Do the Coronavirus Smartphone Tracking Apps Actually Work and Should You Download One to Help?*, REGISTER (Apr. 14, 2020, 2:36 AM), https://www.theregister.com/2020/04/14/coronavirus_phone_app [https://perma.cc/FG2H-RU3R].

app, though it only used this data to ensure citizens did not leave a specific quarantined area.[29] In the United States, Google is the most prominent company to develop technology aggregating population density data to measure social distancing and gatherings, compiling this data into a portal for government officials to peruse.[30]

A major concern inherent to this technology's use is the potential for material inaccuracies and imprecisions. While some government officials are interested in using this data to determine if citizens are complying with social distancing guidelines, GPS data is generally too imprecise to measure a six-foot distance.[31] Further, as seen in the example of Alipay Health Code, this data can be riddled with errors—users of the Alipay app have lodged "countless" complaints of false positives or inexplicable bugs.[32]

Many privacy scholars have "surprised themselves" with their uneasy approval of government location data collection specific to the pandemic context; however, their endorsements have been circumscribed to account for efficacy[33] and other proven metrics.[34] Other concerns related to the storage of that data have arisen from elected officials and other leading privacy groups.[35]

Interaction Data/Bluetooth Apps. One of the most common technologies used to conduct contact tracing programs around the world is Bluetooth. Bluetooth-powered apps interact between enabled devices and track infections, informing individuals who have recently come into close contact with a virus-positive individual in the recent past of their potential exposure.[36] Singapore and other

---

29. *See id.*

30. Tony Romm, *Google Taps Vast Trove of Location Data to Aid Global Effort to Combat Coronavirus*, WASH. POST (Apr. 3, 2020, 2:00 AM), https://www.washingtonpost.com/technology/2020/04/03/google-data-distancing-coronavirus; Geoffrey A. Fowler, *Smartphone Data Reveal Which Americans Are Social Distancing (and Not)*, WASH. POST (Mar. 24, 2020, 3:17 PM), https://www.washingtonpost.com/technology/2020/03/24/social-distancing-maps-cellphone-location.

31. *See* Giglio, *supra* note 22 ("Cohn and others argue that the use of location data in pandemics might not live up to proponents' promises. GPS data are not accurate enough to tell whether someone has been within, say, six feet of an infected person.").

32. *See* McCarthy, *supra* note 28.

33. *See, e.g.*, Giglio, *supra* note 22 (discussing Alan Rozenshtein's tentative approval of location data collection "so long as authorities can show they're effective"); Susan Landau, *Location Surveillance to Counter COVID-19: Efficacy Is What Matters*, LAWFARE (Mar. 25, 2020, 10:46 AM), https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters [https://perma.cc/3Y4T-5QY9].

34. *See, e.g.*, Giglio, *supra* note 22 (quoting Klon Kitchen, a senior fellow at the Heritage Foundation with a long background as a U.S. intelligence officer focused on counterterrorism, as indicating openness "to the idea of expanded surveillance to fight the pandemic—but only if it's conditioned on rigorous constraints and oversight").

35. *See* Letter from Enid Zhou, Open Gov't Counsel, Elec. Privacy Info. Ctr., & John Davisson, Counsel, Elec. Privacy Info. Ctr., to Rachael Leonard, Chief FOIA Officer, Off. of Sci. & Tech. Pol'y (Mar. 24, 2020), https://epic.org/foia/ostp/covid-19/EPIC-20-03-24-OSTP-FOIA-20200324-Request.pdf [https://perma.cc/G88U-5WDW] (relaying a FOIA request from the Electronic Privacy Information Center to the Office of Science and Technology Policy in the White House regarding cell phone location data collection); Letter from Edward J. Markey, Senator, U.S. Senate, to Michael Kratsios, Chief Tech. Officer of the United States, Off. of Sci. & Tech. Pol'y (Mar. 19, 2020), https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20OSTP%20Location%20Data%203.18.20.pdf [https://perma.cc/R5YQ-S237] (indicating concerns with and seeking information on the same program).

36. *See* Tony Romm et al., *Apple, Google Debut Major Effort to Help People Track If They've Come in Contact with Coronavirus*, WASH. POST (Apr. 10, 2020, 4:15 PM), https://www.washingtonpost.com/technology/2020/04/10/apple-google-tracking-coronavirus.

nations have used this technology with great success,[37] and it has made its way to the United States in the form of an unprecedented collaboration between Apple and Google—major rivals in the technology industry.[38] States began to deploy the app in late May 2020.[39]

No strangers to the debate over user privacy, Apple and Google took care to caution the public early that the apps would not track a user's specific location, nor would they reveal an infected person's identity to the platform company or government.[40] While leading scholars in the field have advocated for the mandated use of this app,[41] others have indicated concerns regarding government access to an individual's interactions,[42] the degree to which the data collected is truly anonymized,[43] and the requisite levels of use for the technology to be truly effective.[44] Others have pointed to accuracy issues inherent to Bluetooth technology for this use; for example, such signals can transmit between walls and car doors, though infection is not a risk in that instance.[45] App developers have taken some of these concerns into account, however, and implemented an

---

37. *See* Fathin Ungku, *Singapore Launches Contact Tracing Mobile App to Track Coronavirus Infections*, REUTERS (Mar. 20, 2020, 9:14 AM), https://www.reuters.com/article/us-health-coronavirus-singapore-technolo/singapore-launches-contact-tracing-mobile-app-to-track-coronavirus-infections-idUSKBN2171ZQ (describing TraceTogether, Singapore's official app for contact tracing). Notably, the data TraceTogether collects is encrypted and stored locally on each phone with the app; however, upon request, citizens must submit their logs to the Singaporean health ministry. *Id.* However, the Singaporean government does not retain such data unless the health ministry affirmatively requests it. *See Trace Together Privacy Safeguards*, TRACETOGETHER, https://www.tracetogether.gov.sg/common/privacystatement [https://perma.cc/LF3E-NGAB].

38. *See* Romm et al., *supra* note 36; Zack Whittaker & Darrell Etherington, *Q&A: Apple and Google Discuss Their Coronavirus Tracing Efforts*, TECHCRUNCH (Apr. 13, 2020, 5:18 PM), https://techcrunch.com/2020/04/13/apple-google-coronavirus-tracing [https://perma.cc/7VPJ-FY4V]; McCarthy, *supra* note 28.

39. *See* Romm et al., *supra* note 36; Zac Hall, *Which U.S. States Are Using Apple's Exposure Notification API for COVID-19 Contact Tracing?*, 9TO5MAC (Jan. 16th, 2021, 12:00 AM), https://9to5mac.com/2020/12/07/covid-19-exposure-notification-api-states [https://perma.cc/3RWH-VLVH].

40. *See* Romm et al., *supra* note 36.

41. *See* Stewart Baker, *Singapore's Location App Could Save American Lives*, LAWFARE (Mar. 30, 2020, 4:15 PM), https://www.lawfareblog.com/singapores-location-app-could-save-american-lives [https://perma.cc/6CFE-HV4D] (dismissing privacy advocates' arguments against using apps like TraceTogether); *see also* Giglio, *supra* note 22 (describing TraceTogether and privacy scholars' objections to it, namely government access to information regarding a person's interactions).

42. Giglio, *supra* note 22.

43. *See* McCarthy, *supra* note 28; Giglio, *supra* note 22 (providing an introduction to this technology and issues inherent to anonymization).

44. Adam Vaughan, *There Are Many Reasons Why Covid-19 Contact-Tracing Apps May Not Work*, NEWSCIENTIST (Apr. 17, 2020), https://www.newscientist.com/article/2241041-there-are-many-reasons-why-covid-19-contact-tracing-apps-may-not-work [https://perma.cc/U695-KXLM]; McCarthy, *supra* note 28 (stating 60% of the population has to use this technology for it to be effective); Aradhana Aravindan & Sankalp Phartiyal, *Bluetooth Phone Apps for Tracking COVID-19 Show Modest Early Results*, REUTERS (Apr. 21, 2020, 11:22 AM), https://www.reuters.com/article/us-health-coronavirus-apps/bluetooth-phone-apps-for-tracking-covid-19-show-modest-early-results-idUSKCN2232A0.

45. *See* Romm et al., *supra* note 36 (describing various difficulties and challenges inherent to Bluetooth technology, including its voluntary nature); Giglio, *supra* note 22 ("Bluetooth signals can cut through car doors and walls."); Casey Newton, *Why Bluetooth Apps Are Bad at Discovering New Cases of COVID-19*, VERGE (Apr. 10, 2020, 6:00 AM), https://www.theverge.com/interface/2020/4/10/21215267/covid-19-contact-tracing-apps-bluetooth-coronavirus-flaws-public-health.

anonymized code component into the software that decentralizes infection records and better retains anonymity in a manner similar to blockchain technology.[46]

Code-Scanning. Another method of tracking and tracing infections popular in China, Hong Kong, and Russia is mandated scanning of machine-readable codes, such as QR codes, in public places.[47] This system collects data that is sent to a central server, placing the scanning individual at a specific location and time: if an individual in that same area soon reports her infection, the server manager (in the aforementioned nations' case, the government) can place individuals scanning their codes in the same area and time on notice of potential exposure.[48] To date, only a few government institutions in the United States have utilized this method, though on a much smaller scale.[49]

As is characteristic of many of the nations deploying this technology, however, the opportunity for overbroad surveillance dramatically increases with the collection of this data: rather than serving as an elegant manner of tracking potential exposure, machine code scanning better tracks individuals' movements (with identifiable data), rather than infection.[50] Further, mandated scanning creates a massive data haul—meaning that determining potentially exposed individuals becomes more difficult and time-delayed as the systems managing that data process through potentially affected scanners.[51] Finally, critics note the method is relatively inelegant in predicting exposure as a method of practicality: by providing just one point of reference, the system is not able to determine the length of potential exposure or, depending on the system infrastructure, the relative proximity between the infected individual and other scanners.[52]

Thermal Imaging Camera Installation. Fevers are a common symptom of a coronavirus infection among symptomatic individuals, and many business owners have noted as much in their attempts to protect staff and the public through the purchase and installation of thermal cameras—some of which specialize in scanning temperatures specific to an individual's eyeballs (which camera manufacturers claim is the "closest point to the core of the person's body temperature").[53]

---

46. *See* Darrell Etherington, *MIT Develops Privacy-Preserving COVID-19 Contact Tracing Inspired by Apple's 'Find My' Feature*, TECHCRUNCH (Apr. 9, 2020, 8:48 AM), https://techcrunch.com/2020/04/09/mit-develops-privacy-preserving-covid-19-contact-tracing-inspired-by-apples-find-my-feature [https://perma.cc/MMA7-SSSN]; Douglas Belkin & Kirsten Grind, *MIT Researchers Launch Location-Tracking Effort for the New Coronavirus*, WALL ST. J. (Mar. 27, 2020, 9:27 AM), https://www.wsj.com/articles/mit-researchers-launch-location-tracking-effort-for-the-new-coronavirus-11585315674; McCarthy, *supra* note 28 ("The API documents foresee[] a Bluetooth identifier changing every few minutes with each phone having a single daily tracker that is used to generate a day's worth of identifiers before being changed the next day: the idea being to make it hard-to-impossible to track a specific phone and hard for people to push false claims into the system by generating false identifiers.").

47. McCarthy, *supra* note 28.

48. *See id.*

49. *See Illinois Mobile App*, U. ILL., https://answers.uillinois.edu/illinois/page.php?id=103844 [https://perma.cc/57BS-RSP4].

50. *See* McCarthy, *supra* note 28.

51. *See id.*

52. *See id.*

53. Joseph Cox, *Surveillance Company Says It's Deploying 'Coronavirus-Detecting' Cameras in US*, MOTHERBOARD (Mar. 17, 2020, 3:43 PM), https://www.vice.com/en/article/epg8xe/surveillance-company-deploying-coronavirus-detecting-cameras [https://perma.cc/D7DN-WHTC]; *see* April Glaser, *'Fever Detection' Cameras to Fight Coronavirus? Experts Say They Don't Work*, NBC NEWS (Mar. 27, 2020, 7:01 PM), https://www.nbcnews.com/tech/security/fever-detection-cameras-fight-coronavirus-experts-say-they-don-t-n1170791 [https://perma.cc/43E3-YR6V] (opening with an anecdote involving a Georgia supermarket chain owner who installed such cameras at the entrance to his stores to track potentially-infected customers

Depending on the system, alerts may be transmitted directly to the client, not the scanned individual.[54] Over ten major U.S. companies have promoted their technology as suitable for public health surveillance purposes, and some have pitched police departments and school districts even in small towns on their use.[55] Private companies, however, seem to be the most popular customer of thermal cameras for public health surveillance purposes.[56]

Some privacy advocates have indicated cautious support for thermal camera use during the pandemic, though they note concerns about the potential for surveillance creep extending beyond the pandemic, as well as the technology's potential use during the pandemic in conjunction with facial recognition cameras.[57] Despite the degree of accuracy many camera manufacturers claim,[58] however, some health experts say the technology is not an effective tool for determining who is infected with COVID-19, especially because of the virus's longer incubation period—roughly five days—during which an infected person is asymptomatic but contagious.[59] Further, even setting aside asymptomatic infected individuals, not every symptomatic individual infected with COVID-19 presents with a fever, rendering the technology of limited efficacy.[60]

Facial Recognition Software. Before the pandemic, facial recognition technology was largely circumscribed to the realms of law enforcement and major institutions, the latter of which employ it as a quasi-"digital key" providing an individual with access to a secure facility, like a military base.[61] However, facial recognition systems—many of which rely heavily on artificial intelligence or machine learning for efficient matches to an existing image database—grew in popularity in the

---

with an internal head temperature of 100.4 degrees or higher); Giglio, *supra* note 22 ("Other companies have been marketing thermal-imaging cameras to the government that, while of dubious utility, raise further privacy issues.").

54. *See* Cox, *supra* note 53.

55. Glaser, *supra* note 53 (detailing one company's pitch to the Las Vegas Police Department); Gregory Barber, *Schools Adopt Face Recognition in the Name of Fighting Covid*, WIRED (Nov. 3, 2020, 7:00 AM), https://www.wired.com/story/schools-adopt-face-recognition-name-fighting-covid (reporting on the Rio Rancho, New Mexico school board's purchase of thermal cameras and facial recognition technology).

56. *See* Glaser, *supra* note 53 (listing major companies using this technology, such as Wynn resorts, and camera companies' backlog of orders).

57. *See* Giglio, *supra* note 22 (discussing Alan Rozenshtein's cautious support for thermal camera use); Alan Z. Rozenshtein, *Government Surveillance in an Age of Pandemics*, LAWFARE (Mar. 23, 2020, 4:20 PM), https://www.lawfareblog.com/government-surveillance-age-pandemics [https://perma.cc/E42D-NLGG]; Glaser, *supra* note 53 (describing an ACLU lawyer's cautious support for the technology, provided public health officials deem it effective).

58. *See, e.g.*, Cox, *supra* note 53 ("The representative claimed that the software is accurate within half a degree and that it detects a dozen different parts on the body. They added the system has 'no facial recognition, no personal tracking.'").

59. *See, e.g.*, Glaser, *supra* note 53.

60. *See id.* ("'The big problem is that not everyone develops a fever. The vast majority of cases are mild to moderate,' said Dr. Joseph Fair, a virologist and epidemiologist, referring to COVID-19. 'And then we have asymptomatic people as well that are very infectious.[] []Temperature checks are things that we mostly do out of an abundance of caution, but they're mostly a visual measure that makes you feel better,' Fair said. 'It makes you feel like you're going through some kind of screening but they have very limited effectiveness.'").

61. *See* Chris Baraniuk, *Why Covid May Mean More Facial Recognition Tech*, BBC NEWS (Dec. 4, 2020), https://www.bbc.com/news/business-54959193 [https://perma.cc/PJ7M-LWSQ] (detailing one facial recognition technology company's recent success in a competitive bid process to install facial recognition access control systems at two U.S. Air Force bases in a move "designed specifically to reduce contact between people at the bases").

early days of the pandemic, particularly for countries utilizing QR code scanning systems to track citizens' movements.[62]

While many companies developing this technology paused some operations in the summer of 2020 in support of racial justice movement activists' concerns regarding the technology (and its abuse in the hands of federal and local law enforcement),[63] its use has persisted in limited contexts.[64] As racial justice activists have noted for years, facial recognition technology is rife with bias and accuracy issues, the latter of which being exacerbated by face covering use.[65] Notably, before the pandemic even began, members of Congress expressed rare bipartisan opposition to facial recognition technology, citing accuracy issues and potential encroachment on constitutionally protected civil liberties.[66] Even conservative Republicans called for legislation regulating the technology, though it is already in use in jurisdictions across the country.[67] Some cities have even banned its use.[68]

In the context of the pandemic, however, some privacy advocates have indicated cautious support for the expanded use of facial recognition software.[69] However, its use in the United States in

---

62. *See* Melissa Zhu, *What Is Facial Recognition, and Why Is It More Relevant than Ever During the Coronavirus Pandemic?*, S. CHINA MORNING POST (Nov. 18, 2020, 6:00 AM), https://www.scmp.com/tech/policy/article/3108742/what-facial-recognition-and-why-more-relevant-ever-during-covid-19 [https://perma.cc/2YRX-VBBU].

63. *See* Karen Weise & Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, N.Y. TIMES (June 10, 2020), https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html (initiating a one-year pause on police use of Amazon's facial recognition software, Rekognition); Steven Musil, *IBM to Withdraw from Facial Recognition Market out of Profiling Fears*, CNET (June 8, 2020, 4:40 PM), https://www.cnet.com/news/ibm-to-withdraw-from-the-facial-recognition-market [https://perma.cc/H8JS-K37K] (reporting IBM's withdrawal from the "general-purpose facial recognition market" in support of racial justice activists); Jay Greene, *Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020, 2:30 PM), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ (reporting Microsoft's intention to pause sale of its facial recognition systems to police forces until federal legislation regulates the technology). *See generally* Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html (reporting that facial recognition technology errors increase in proportion to the darkness of a person's skin tone); Alfred Ng, *Facial Recognition Has Always Troubled People of Color. Everyone Should Listen*, CNET (June 12, 2020, 5:00 AM), https://www.cnet.com/news/facial-recognition-has-always-troubled-people-of-color-everyone-should-listen [https://perma.cc/VE7W-PEFM].

64. *See infra* note 70 and accompanying text.

65. *See* Ng, *supra* note 63.

66. *See* Drew Harwell, *Both Democrats and Republicans Blast Facial-Recognition Technology in a Rare Bipartisan Moment*, WASH. POST (May 22, 2019, 4:09 PM), https://www.washingtonpost.com/technology/2019/05/22/blasting-facial-recognition-technology-lawmakers-urge-regulation-before-it-gets-out-control (relaying the statements of leaders on the House Committee on Oversight and Reform in opposition to the technology). Notably, members drew parallels between the technology's potential use in the United States to its use in China, "where it is critical to the government's systems of public monitoring and social control." *Id.*

67. *See id.* (citing then-Representative Mark Meadows, a Republican from North Carolina, in his calls to restrain the technology before "it gets out of control").

68. *See* Corinne Reichert, *Facial Recognition Banned in Another City*, CNET (July 17, 2019, 11:41 AM), https://www.cnet.com/news/facial-recognition-banned-in-another-city [https://perma.cc/V7ED-RW59] (reporting on Oakland, California's adoption of a city ordinance banning police forces from using facial recognition technology, following the lead of Somerville, Massachusetts and San Francisco, California).

69. *See* Giglio, *supra* note 22 (discussing Alan Rozenshtein's cautious support for expanded use of facial recognition software); Rozenshtein, *supra* note 57 (same).

combating the pandemic appears to remain limited to the contexts of schools and workplaces as a means of exacting discipline.[70]

Social Media Data-Scraping Technology. A new means of furthering public health surveillance already underway at the CDC involves the application of machine learning to social media websites, in which software "scrapes" status updates, photos, and other data from public social media accounts and analyzes it for health-related information, all for the end of determining outbreaks and infections in areas where testing may be lacking or reporting may be unreliable.[71] When utilized in the pandemic, the program scans specifically for complaints related to common symptoms of COVID-19, such as respiratory issues or fever, to determine the location of outbreaks and, potentially, to map the virus's aggregate presentation on different classes of individuals (e.g., by gender and/or age).[72] Notably, this technology played a critical role in determining the initial severity of the coronavirus for WHO officials in December 2019, as the Chinese government downplayed the virus's spread in the earliest days and silenced infectious disease leaders' calls for alarm.[73]

In some cases, the federal government has already entered contracts and has begun the process of scraping information to establish various metrics of interests. For example, data collection company Crimson Hexagon has a $30,000 contract with the Centers for Disease Control and Prevention (CDC) to utilize its "social listening" tools, "meaning it scrapes public Facebook, Instagram and Twitter posts in part to gauge sentiment."[74] This contract predated the first case of COVID-19.[75]

While this technology played a critical role in documenting the initial spread of the virus in China, a famously controlling nation, it is not without faults—scholars specializing in the nexus of these phenomena have noted that novel diseases like COVID-19 can be difficult to track, particularly when the host of symptoms characterizing it differ between infected individuals and may overlap with less serious maladies like seasonal allergies.[76] However, public health scholars have indicated cautious enthusiasm for the proliferation of this technology, particularly as the contours of the virus have come into greater detail.

Internet of Things (IoT) Technology. While "smart" technology is now commonplace to the American experience—ordinary household appliances like ovens and dishwashers now come equipped with WiFi, and millions of Americans now employ digital "assistants," like the Amazon Alexa, in their home—health equipment like "smart thermometers" may now play a critical role in mapping the

---

70. *See* Barber, *supra* note 55 (detailing the proliferation of this technology in schools, first as a means of combatting gun violence, and now as an add-on to thermal camera technology and independently to discipline students); Ashleigh Webber, *PwC Facial Recognition Tool Criticised for Home Working Privacy Invasion*, PERSONNEL TODAY (June 16, 2020), https://www.personneltoday.com/hr/pwc-facial-recognition-tool-criticised-for-home-working-privacy-invasion [https://perma.cc/4WDY-8L5E] (discussing accounting company PricewaterhouseCoopers's development of facial recognition technology utilizing employees' webcams to log absences from their computer screens while working remotely).

71. *See* Will Knight, *How AI Is Tracking the Coronavirus Outbreak*, WIRED (Feb. 8, 2020, 7:00 AM), https://www.wired.com/story/how-ai-tracking-coronavirus-outbreak (detailing social media scraping technology, such as BlueDot, and its use with machine learning technology to track viral outbreaks).

72. *See id.*

73. *See id.*

74. Grind et al., *supra* note 17.

75. *See id.*

76. *See* Knight, *supra* note 71.

spread of COVID-19 before public health officials are aware of an outbreak.[77] The *New York Times* reported specifically on one such "smart thermometer," the Kinsa, in its mapping of the 2018 flu season[78] and now COVID-19, where thermometer company Kinsa Health showed fever spikes in South Florida days before the CDC, which relies on weekly reports from doctor's offices and hospitals to determine infection levels in a given area.[79] Given the preponderance of fevers as a symptom of COVID-19 infection, this technology provides a rough guideline to potential outbreaks in real time.

Public health experts and medical researchers have expressed enthusiasm for the use of this technology, noting that being able to predict the spread of fever-based diseases up to two weeks earlier than the CDC can assist the CDC and health resource management companies in deploying personal protective equipment (PPE) and testing kits, among other medical necessities.[80] However, the federal government has not contracted directly with Kinsa or any other smart thermometer company, though state governments have considered its use.[81] Further, while medical experts have indicated support for the technology, critics have pointed to the relatively small sample size Kinsa offers as cause for skepticism.[82]

Legal Precedent and Issues

Federalism has played a key role in the United States' response to the pandemic, largely due to President Donald J. Trump's choice to cede much of the federal authority guiding such management to state governments.[83] While the federal government (and thus, federal law) has a role to play, States have been empowered to craft responses as they see fit, creating conflicting precedents surrounding the collection and use of citizens' personally identifiable information

---

77. *See* Donald G. McNeil Jr., *Can Smart Thermometers Track the Spread of the Coronavirus?*, N.Y. TIMES (Mar. 18, 2020), https://www.nytimes.com/2020/03/18/health/coronavirus-fever-thermometers.html.

78. *See* Donald G. McNeil Jr., *'Smart Thermometers' Track Flu Season in Real Time*, N.Y. TIMES (Jan. 16, 2018), https://www.nytimes.com/2018/01/16/health/smart-thermometers-flu.html.

79. *See* McNeil, *supra* note 77.

80. *Id.*

81. *See* Marie McCullough, *Smart Thermometers Could Help Track COVID-19 Surge in Philadelphia — If Used in a Smart Way*, PHILA. INQUIRER (Nov. 17, 2020), https://www.inquirer.com/health/coronavirus/covid-19-outbreaks-kinsa-thermometers-track-fevers-early-warning-philadelphia-20201117.html ("[Philadelphia's] health department has used federal pandemic aid to buy [smart] thermometers that could be targeted to poorer zip codes, where COVID-19 has taken a disproportionate toll.").

82. *See* Jane C. Hu, *So About That Thermometer Data That Says Fevers Are on the Decline . . .* , SLATE (Apr. 6, 2020, 4:20 PM), https://slate.com/technology/2020/04/kinsa-smart-thermometer-data-fevers-covid19.html [https://perma.cc/E2TU-LFKL].

83. *See* Nicholas & Gilsinan, *supra* note 4. *But cf.* Dartunorro Clark, *Trump Tells Governors He Is Setting New Coronavirus Social Distancing Guidelines*, NBC NEWS (Mar. 26, 2020, 2:37 PM), https://www.nbcnews.com/politics/white-house/trump-tells-governors-he-setting-new-coronavirus-guidelines-n1169751 [https://perma.cc/PP23-ZXDY] (relaying President Trump's announcement of new guidelines allowing his administration to identify "high-risk, medium-risk and low-risk" counties in an effort to assist governors and local officials as they determine whether to strengthen or relax social distancing mandates); Camille Caldera, *Fact Check: Governors, President Both Responsible for Pandemic Response*, USA TODAY (Aug. 19, 2020, 9:41 PM), https://www.usatoday.com/story/news/factcheck/2020/08/19/fact-check-governors-president-both-responsible-pandemic-response/3296998001 [https://perma.cc/EE42-2J7Y]; Betsy Woodruff Swan, *DOJ Seeks New Emergency Powers amid Coronavirus Pandemic*, POLITICO (Mar. 21, 2020, 1:01 PM), https://www.politico.com/news/2020/03/21/doj-coronavirus-emergency-powers-140023 [https://perma.cc/6BWY-Y8JB].

(PII). This section will explore both federal and state laws relevant to this conversation as they govern state-sanctioned collection of this data.

Federal Law

Federal laws governing privacy and PII are largely limited to the pre-internet era, compounding confusion and ambiguity as innovative technologies enter the marketplace. There is no one federal law governing privacy writ large; rather, data collection and privacy are governed by a patchwork of topically-focused (or "sector-specific") laws held in check by various constitutional amendments.[84] When private companies collect users' data in the provision of a good or service, the predominant privacy concern centers on how that company chooses to use that data; if its sale or transfer is not prohibited by one of the aforementioned sector-specific laws (or is not unfair, deceptive, or abusive under the framework established in the Federal Trade Commission Act[85]), a company may permissibly sell or transfer that data to a data "broker" without the consumer's knowledge or consent, feeding into a secondary market of PII.[86] However, a transfer of PII to the federal government implicates a number of federal laws, several of which are particular to this context.

Broadly, the present lack of legal controls guiding how the federal government may permissibly use collected data remains an open issue.[87] Theoretically, location information collected during the pandemic could later shift hands to the IRS, were an individual to owe back taxes, or the FBI;[88] such a transfer is expressly contemplated by the text of the Privacy Act of 1974.[89]

While Congress has rejected proposals to create a national identification card[90] despite technology companies' offers to develop the supporting software for free,[91] other proposed systems remain in the liminal space between authorization and prohibition. The list below details the legal authorities guiding the federal legal landscape in this regard.

The U.S. Constitution. The constitutional "right to privacy" enumerated in relevant Supreme Court case law is dedicated to curbing government intrusions into citizens' private lives, but not private companies' intrusions.[92] However, when private companies provide data to the federal government, the Constitution and various amendments—predominantly the Fourth—come into play, further

84. *See generally* STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 1, 57 (2019) ("Despite the rise in interest in data protection, the legislative paradigms governing cybersecurity and data privacy are complex and technical, and lack uniformity at the federal level.").

85. 15 U.S.C. §§ 41–58.

86. *See* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 11–13 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/G6MB-WRJT].

87. Timberg & Harwell, *supra* note 17.

88. *See id.* (quoting Professor Albert Girardi as discussing this very possibility).

89. 5 U.S.C. § 552a.

90. 6 U.S.C. § 554.

91. *See* Sumner Lemon, *Ellison Offers Free Software for National ID*, COMPUTERWORLD (Sept. 24, 2001, 12:00 AM), https://www.computerworld.com/article/2583197/ellison-offers-free-software-for-national-id.html [https://perma.cc/RHK9-3QUC].

92. *See* MULLIGAN ET AL., *supra* note 84, at 2.

delineating this right's contours.[93] For example, in *Carpenter v. United States*,[94] the Supreme Court held the Fourth Amendment's privacy protections bar governments from accessing some information shared with a third party, such as cell phone location data, because while the third party doctrine generally holds that individuals do not have a reasonable expectation of privacy in information they share with a third party, they do "maintain[] a legitimate expectation of privacy in the record of [their] physical movements as captured through [their cell phone]."[95] Governments must thus obtain a warrant from a cell phone company to obtain a citizen's location data as captured by his cell phone—meaning the GPS location data transfer contemplated as a method of pandemic management presents a modified version of the *Carpenter* facts, given their anonymized presentation and the context in which the data is sought.

The Supreme Court has also contemplated a right to "liberty"—a more general privacy interest that protects citizens even outside the context of search and seizure.[96] In the 1977 case *Whalen v. Roe*,[97] the Court detailed two kinds of interests covered by the right to privacy: "the individual interest in avoiding disclosure of personal matters, and . . . the interest in independence in making certain kinds of important decisions."[98] The first of these could include information privacy, as the Court expressly contemplated in *NASA v. Nelson*[99] in 2011.[100]

Open questions remain as to the limits the Fourth Amendment might impose in "administrative" or "special needs" contexts, like public health concerns during a pandemic.[101] *Whalen* itself arose in the context of medical care; there, "physicians and patients challenged a New York law that required the recording of the names and addresses of all persons who had obtained certain drugs for which there was both a lawful and unlawful market."[102] While the Court acknowledged the disclosure's threat to impair the interest in the non-disclosure of private information, it upheld the law as an "essential part of modern medical practice."[103] Other challenges under the "liberty" right have also failed, lending to murky contours of an otherwise undefined right.

---

93. *See id.* at 5 (footnotes omitted) ("Some provisions protect privacy in a relatively narrow sphere, such as the Third Amendment's protection against the quartering of soldiers in private homes or the Fifth Amendment's protection against self-incrimination. The most general and direct protection of individual privacy is contained in the Fourth Amendment, which states that '[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .'" (quoting U.S. CONST. amend. IV)).

94. 138 S. Ct. 2206 (2018).

95. *Id.* at 2217 (citing United States v. Miller, 425 U.S. 435, 443 (1976); Smith v. Maryland, 442 U.S. 735, 741

(1979)).

96. *See* Whalen v. Roe, 429 U.S. 589, 598–600 (1977); MULLIGAN ET AL., *supra* note 84, at 6 (providing a background to this right and tying it to data protection and privacy).

97. 429 U.S. 589 (1977).

98. *Id.* at 599–600 (footnote omitted).

99. 562 U.S. 134 (2011).

100. *See id.* at 146 ("But no other decision has squarely addressed a constitutional right to informational privacy."); *id.* at 146 n.9 (listing state and local decisions interpreting *Whalen* and like cases specific to the context of information privacy).

101. Generally, routine administrative searches require consent or a warrant. *See* Camara v. Mun. Ct. of City & Cnty. of S.F., 387 U.S. 523 (1967). However, Supreme Court case law has not yet addressed the question of warrantless administrative searches for public health surveillance purposes during a national emergency, like a pandemic. *See* Rozenshtein, *supra* note 57.

102. MULLIGAN ET AL., *supra* note 84, at 6 (citing *Whalen*, 429 U.S. at 591).

103. *Whalen*, 429 U.S. at 602, 604–05.

The Stored Communications Act. The Stored Communications Act[104] (SCA) provides an exception permitting companies to voluntarily share data with the government in the event of an emergency.[105] Though the government may not mandate that companies provide this data outside of a criminal investigation,[106] the SCA provides the legal framework through which covered companies—specifically, electronic communication service providers or internet service providers—may disclose critical information to the federal government.

Emergency Powers Acts. Under the National Emergencies Act[107] and the Robert T. Stafford Disaster Relief and Emergency Assistance Act,[108] the President retains expansive powers when he declares a national emergency, which then-President Trump did on March 13, 2020.[109] By activating both with his declaration, the President rendered more than 120 emergency provisions effective, including the power to deploy troops or to convert commissioned corps of the public health service to military service.[110]

However, the President is not the only federal executive with the power to make emergency designations with broad effects. Under the Public Health Service Act,[111] the Secretary of the Department of Health and Human Services may also declare a public health emergency, triggering the broad authority to act "as may be appropriate to respond."[112]

Though all of these laws provide broad powers, little description or detail exists in the legislative text itself. Instead, these laws largely provide the supportive framework for broadened powers under other laws, like the Stored Communications Act.[113]

State and Local Law

President Trump's express choice to invoke federalism has resulted in the management and response to the COVID-19 pandemic occurring almost entirely on the state and local level.[114] Contact tracing and other innovative technological responses have thus become functions of state

---

104. 18 U.S.C. §§ 2701–2712.

105. *See* 18 U.S.C. § 2702 (stating that while generally entities providing electronic communication services may not divulge the contents of an electronic communication, an exception exists specifically if the entity provides those communications "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency").

106. 18 U.S.C. § 2703.

107. 50 U.S.C. §§ 1601–1651.

108. 42 U.S.C. §§ 5121–5207 (2018).

109. *See* Charlotte Butash, *What's In Trump's National Emergency Announcement on COVID-19?*, LAWFARE (Mar. 14, 2020, 7:45 PM), https://www.lawfareblog.com/whats-trumps-national-emergency-announcement-covid-19 [https://perma.cc/YS6P-M4TM].

110. Kim, *supra* note 8.

111. Pub. L. No. 78-410, 58 Stat. 682 (1944).

112. 42 U.S.C. § 247d .

113. *See, e.g.*, *supra* notes 104–106 and accompanying text.

114. *See* Nicholas & Gilsnian, *supra* note 4. President Trump has defended this delegation of power as a mandate set forth by the Tenth Amendment, which constitutional scholars interpret as ceding "police powers" to the States. *See* William A. Galston, *Trump or Governors: Who's the Boss?*, BROOKINGS INST. (Mar. 25, 2020), https://www.brookings.edu/blog/fixgov/2020/03/25/trump-or-governors-whos-the-boss [https://perma.cc/V6ZT-WS5X]. Complicating matters, however, is the high cost of hiring, training, and maintaining an effective contact tracing program—many States do not have the funds necessary to start large tracing programs, and most state departments of public health were already underfunded prior to the pandemic. *See* Aschwanden, *supra* note 18.

constitutions, legislation, and executive orders, where special interests may run roughshod over measured lawmaking.[115] Just as the federal government has engaged in conversations with technology companies to aggregate this data, these companies have also pitched state and local governments.[116]

However, many state laws already permit state governments to mandate citizens download certain tracking apps. As Stewart Baker discussed in a recent post for *Lawfare*, forty States enacted versions of a model public health emergency law in the aftermath of September 11 providing governors with "explicit authority to issue orders seizing 'materials and facilities as may be reasonable and necessary to respond to the public health emergency,'" with "materials and facilities" including electronic communication devices such as cell phones.[117] Baker continues:

> In fact, if push comes to shove, the governors likely have authority to require that residents of their states activate the app. The law grants individual states the emergency authority to conduct "any diagnostic or investigative analyses necessary to prevent the spread of disease." And, since Apple and Android know which apps we've activated, they could be ordered to identify those who haven't registered for contact tracing. The federal law prohibiting disclosure of subscriber information to governments without a subpoena contains an express exception for "an emergency involving danger of death or serious physical injury to any person."[118]

While forty States have enacted versions of the model law, such a move would be without precedent.[119]

Still, States have encountered resistance to some of their COVID-19 management actions from a privacy paradigm. North Carolina, for example, has suffered disproportionately high infection rates among its Hispanic community, with some attributing the issue to lacking testing in the community for fear of mandated immigration status disclosure.[120] New York and California's new

---

115. *See* Molly Jackman, *ALEC's Influence over Lawmaking in State Legislatures*, BROOKINGS INST. (Dec. 6, 2013), https://www.brookings.edu/articles/alecs-influence-over-lawmaking-in-state-legislatures [https://perma.cc/TGZ9-NJHU] (describing the American Legislative Exchange Council's disproportionate influence over state legislatures across the country).

116. *See* Grind et al., *supra* note 17.

117. *See* Baker, *supra* note 41; THE CTR. FOR L. & THE PUB.'S HEALTH AT GEO. & JOHNS HOPKINS UNIVS., THE MODEL STATE EMERGENCY HEALTH POWERS ACT (2001), https://www.aapsonline.org/legis/msehpa2.pdf [https://perma.cc/D532-R8F5]; *Q&A on the Model State Emergency Health Powers Act*, AM. C.L. UNION, https://www.aclu.org/other/model-state-emergency-health-powers-act [https://perma.cc/N96D-T7A7] (expressing concerns regarding the breadth of the Act in its early days); Lawrence O. Gostin, *The Model State Emergency Health Powers Act: Public Health and Civil Liberties in a Time of Terrorism*, 13 HEALTH MATRIX 3, 5 (2003) (stating that as of publication, thirty-nine States and the District of Columbia had enacted, or would soon enact, a version of the Act); *see also* Giglio, *supra* note 22 (discussing Baker's assertions).

118. Baker, *supra* note 41 (citing 18 U.S.C. § 2702).

119. *See* Giglio, *supra* note 22 (quoting Baker as stating so).

120. *See* Chas Kissick, *Privacy Issues at the Heart of North Carolina's Coronavirus Response*, LAWFARE (Oct. 15, 2020, 2:15 PM), https://www.lawfareblog.com/privacy-issues-heart-north-carolinas-coronavirus-response [https://perma.cc/5E5Y-LKG8] ("In fact, privacy concerns are pulling the response in three directions. First, local authorities are fighting over access to test results and contact-tracing data. Second, fear of data leakage—whether legal (such as from the Department of Health and Human Services or law enforcement) or illegal—is impairing contact tracing, especially in the Hispanic community. And finally, well-intentioned concern for privacy is hindering research on convalescent plasma and its utility as a treatment or its indirect use for vaccine and treatment development."); Hannah Critchfield, *Undocumented, Uninsured and Worried About ID Requirements? You Can Still Get Free COVID-19 Tests*, N.C. HEALTH NEWS (July 20, 2020), https://www.northcarolinahealthnews.org/2020/07/20/undocumented-uninsured-and-worried-about-id-requirements-you-can-still-get-free-covid-19-tests [https://perma.cc/6W64-ENLR].

privacy laws have complicated the use of the management tools state leaders wish to utilize in addressing the pandemic,[121] and reactive legislation has made inroads in the New York State Senate.[122]

Conclusion

Innovative technology offers a myriad of possibilities for governments all over the world to track the spread of COVID-19, better facilitating pandemic management and response through the analysis of this more readily available information. Though these advances offer great promise, the collection and retention of this data poses new challenges to the privacy law bar, with the potential to change privacy norms long after the pandemic's end.

121. *See* Roxane A. Polidora et al., *New Privacy Laws in California and New York Are on a Collision Course with the COVID-19 Technology Boom*, PILLSBURY (July 15, 2020), https://www.pillsburylaw.com/en/news-and-insights/ccpa-ny-shield-privacy-covid-19.html [https://perma.cc/6XLM-WRYZ].

122. *See* Kevin Thomas, *COVID-19 Data Privacy Legislation Passes New York State Senate*, N.Y. STATE SENATE (July 23, 2020), https://www.nysenate.gov/newsroom/press-releases/kevin-thomas/covid-19-data-privacy-legislation-passes-new-york-state-senate [https://perma.cc/52PQ-ARU7].

Panelists

Gregory T. Nojeim. Gregory T. Nojeim is a Senior Counsel and Director of the Freedom, Security, and Technology Project at the Center for Democracy & Technology (CDT), a Washington, D.C. non-profit public policy organization dedicated to keeping the internet open, innovative and free. He specializes in protecting privacy in the digital age against intrusion by the U.S. government, and he is a recognized expert on the USA PATRIOT Act, the Foreign Intelligence Surveillance Act, the Electronic Communications Privacy Act, and the application of the Fourth Amendment to electronic surveillance in the national security, intelligence, and criminal arenas.

Mr. Nojeim directs CDT's initiatives that respond to the 2013 disclosures about NSA surveillance and was engaged in CDT's successful efforts to promote the USA FREEDOM Act of 2015, the bill that ended bulk collection of telephone call records under the PATRIOT Act. Mr. Nojeim also spearheaded CDT's initiative to promote judicial supervision of surveillance conducted under 2008 amendments to the Foreign Intelligence Surveillance Act. He is the lead strategist for CDT's cybersecurity work, having testified in both the House and Senate on the impact of cybersecurity proposals on privacy, civil liberties, and technology innovation. He is also deeply involved in a multi-year, broad-based project to update the Electronic Communications Privacy Act (ECPA) to account for new technologies and is the President of Digital 4th, a coalition formed around ECPA reform.

Mr. Nojeim sits on the Board of Directors of the Global Network Initiative, a multi-stakeholder group of companies, human rights and press freedom organizations, academics, and investors who collaborate to advance freedom of expression and privacy in the information and communications technology sector. He is a member of the Data Privacy and Integrity Advisory Committee, which advises the Department of Homeland Security on privacy matters. As Co-Chair of the Coordinating Committee on National Security and Civil Liberties of the American Bar Association's Section on Individual Rights and Responsibilities, he was one of the lead drafters of the ABA's 2007 policy on the state secrets privilege.

Prior to joining CDT in 2007, Mr. Nojeim was the Associate Director and Chief Legislative Counsel of the ACLU's Washington Legislative Office. At the ACLU, he analyzed the civil liberties implications of terrorism, national security, immigration, and informational privacy legislation. Mr. Nojeim also served for four years as the Director of Legal Services of the American-Arab Anti-Discrimination Committee (ADC), and conducted much of ADC's work on immigration, civil rights, and human rights. He was an attorney with the Washington, D.C. law firm of Kirkpatrick & Lockhart (now K&L Gates) where he specialized in mergers and acquisitions, securities law, and international trade.

Mr. Nojeim graduated from the *University of Rochester* in 1981 with a BA in Political Science. He received his JD from the *University of Virginia* in 1985, where he sat on the Editorial Board of the *Virginia Journal of International Law.*

Mr. Nojeim's pertinent publications in this space include:

- Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SEC. L. & POL'Y 119 (2010).
- Ira S. Rubenstein, Gregory T. Nojeim, & Ronald D. Lee, *Systematic Government Access to Personal Data: A Comparative Analysis*, 4 INT'L DATA PRIVACY L. 96 (2014).
- Gregory T. Nojeim, *Financial Privacy*, 17 N.Y.L. SCH. J. HUM. RTS. 81 (2000).
- Gregory T. Nojeim, *Cybersecurity: Ideas Whose Time Has Not Come—and Shouldn't*, 8 INFO. SOC'Y: J.L. & POL'Y 408 (2012).

Professor Matt Perault. Professor Perault is an Associate Professor of the Practice at the *Duke University Sanford School of Public Policy*, and the Director of *Duke*'s Center on Science & Technology

Policy. Prior to entering academia, Professor Perault served as a director of public policy at Facebook, where he led the company's global public policy planning efforts on issues such as competition, law enforcement, and human rights, and oversaw public policy for WhatsApp, Oculus, and Facebook Artificial Intelligence Research. Before joining Facebook, Professor Perault was Counsel for the Congressional Oversight Panel, worked as a consultant at the World Bank, and served as a law clerk for the U.S. District Court for the District of Columbia. Professor Perault holds a law degree from *Harvard Law School*, a Master's degree in Public Policy from the *Duke University Sanford School of Public Policy*, and a Bachelor's degree in political science from *Brown University*.

Professor Perault's pertinent publications in this space include:

- Matt Perault, *Section 230: A Reform Agenda for the Next Administration*, DAY ONE PROJECT, https://www.dayoneproject.org/post/section-230-reform (last visited Jan. 1, 2021).

Professor Perault's recent contributions to the scholarship include:

- Ashley Gold, *The People Trying to Get in Biden's Head on Holding Tech Accountable*, AXIOS (Oct. 26, 2020), https://www.axios.com/the-people-trying-to-get-in-bidens-head-on-holding-tech-accountable-383b5866-164d-42aa-8531-0c24ff8a8f30.html (describing Professor Perault's leadership on the Day One plan, including suggested criminalization of certain online speech such as intentional voter suppression).
- *Tackling Technology's Unintended Consequences*, DUKE TODAY (Dec. 12, 2019), https://today.duke.edu/2019/12/tackling-technologys-unintended-consequences [https://perma.cc/Z6DE-2JSN] (profiling Professor Perault's work as the director of Duke's new Center on Science & Technology Policy).

Dr. Anne L. Washington. Dr. Washington is a Public Interest Technologist serving as an Assistant Professor of Data Policy at the *NYU Steinhardt School*. Her expertise on public sector information currently addresses the emerging governance needs of data science. The National Science Foundation has funded her research multiple times, including through a prestigious 5-year NSF CAREER grant on open government data. Her data-intensive projects draw on both interpretive research methods and computational text analysis.

She holds an undergraduate degree from *Brown University*, a graduate degree from *Rutgers University*, and a doctorate in Information Systems and Technology Management from *The George Washington University School of Business*. Prior to completing her doctorate, Dr. Washington had extensive work experience with the Congressional Research Service at the Library of Congress, Barclays Global Investors, and Apple Computer. Professor Washington serves on the Advisory Boards of the Electronic Privacy Information Center (EPIC) and the Open Government Foundation.

Dr. Washington's recent contributions to this area include:

- Anne L. Washington & Lauren Rhue, *Pandemic Privacy in the Workplace*, POINTS, (June 17, 2020), https://points.datasociety.net/pandemic-privacy-in-the-workplace-a3cb92baffc [https://perma.cc/DSZ2-CRU9] (outlining the potential dangers of new technologies that might expose employee's COVID-19 status).
- Anne L. Washington, *Government Information Policy in the Era of Big Data*, 31 REV. POL'Y RSCH. 319 (2014) (examining the policy implications of using U.S. federal public sector information in big data projects).

Professor Jennifer Daskal. Professor Daskal is a Professor and Faculty Director of the Tech, Law & Security Program at *American University Washington College of Law*, where she teaches and writes in

the fields of cyber, national security, criminal, and constitutional law. From 2009–2011, Professor Daskal worked as the counsel to the Assistant Attorney General for National Security at the Department of Justice. Prior to joining the DOJ, Professor Daskal was senior counterterrorism counsel at Human Rights Watch, worked as a staff attorney for the Public Defender Service for the District of Columbia, and clerked for the Honorable Jed S. Rakoff. She also spent two years as a national security law fellow and adjunct professor at *Georgetown University Law Center*. From 2016–2017, she was an Open Society Institute Fellow working on issues related to privacy and law enforcement access to data across borders. She is currently a New America ASU Future of Security Fellow.

Professor Daskal's scholarship has appeared in the *Yale Law Journal*, *University of Virginia Law Review*, *University of Pennsylvania Law Review*, *Vanderbilt Law Review, Stanford Law Review Online*, and *Harvard Journal of National Security Law*, among other places. She has published numerous op-eds, including in the *New York Times*, *Washington Post*, *The Atlantic*, and *Slate* and has appeared on BBC, C-SPAN, MSNBC, and NPR, among other media outlets. She is an Executive Editor of the *Just Security* blog, an Advisory Board Member of the Third Way's Cyber Enforcement Initiative, and an Executive Editor of the *Journal on National Security Law and Policy*.

Professor Daskal's recent contributions to this area include:

- Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018).
- Jennifer Daskal, *Notice and Standing in the Fourth Amendment: Searches of Personal Data*, 26 WM. & MARY BILL RTS. J. 437 (2017).
- Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SEC. L. & POL'Y 473 (2016).
- Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015).
- Jennifer Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327 (2014).

Event Run of Show

The entire event will be hosted virtually on Zoom. All times are Eastern Standard.

Day One: Thursday, February 4, 2021

Opening Remarks
5:00–5:05 p.m.: Robert Dinerstein, *AUWCL* Acting Dean, will welcome attendees and give a brief history of the event.
5:05–5:15 p.m.: Kiran Jeevanjee, *AULR* Senior Symposium Editor, and John Verderame, *AULR* Editor-in-Chief, will give opening remarks.

Surveillance & Privacy in the Pandemic
5:15–5:20 p.m.: Panelist introductions
5:20–6:05 p.m.: Panel discussion
6:05–6:15 p.m.: Audience Q&A

Contact Tracing & Innovative Technological Responses
6:30–6:35 p.m.: Panelist introductions
6:35–7:20 p.m.: Panel discussion
7:20–7:30 p.m.: Audience Q&A

Closing Remarks
7:30–7:35 p.m.: Kiran Jeevanjee, *AULR* Senior Symposium Editor, will deliver end-of-day closing remarks.

Day Two: Friday, February 5, 2021

Opening Remarks
10:00–10:15 a.m.: John Verderame, *AULR* Editor-in-Chief, will deliver opening remarks and preview the day's events.

Evolution of Healthcare Privacy
10:15–10:20 a.m.: Panelist introductions
10:20–11:05 a.m.: Panel discussion
11:05–11:15 a.m.: Audience Q&A

Lessons Learned: The Future of Digital Privacy
11:30–11:35 a.m.: Panelist introductions
11:35 a.m.–12:20 p.m.: Panel discussion
12:20–12:30 p.m.: Audience Q&A

Closing Remarks
12:30–12:35 p.m.: John Verderame, *AULR* Editor-in-Chief, will close out the event with some brief closing remarks.