Boston University School of Law
Scholarly Commons at Boston University School of Law

Faculty Scholarship

9-2020

Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis

Tiffany Li
Boston University School of Law

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship

 Part of the Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

Tiffany Li, *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*, (2020).
Available at: https://scholarship.law.bu.edu/faculty_scholarship/973

This Working Paper is brought to you for free and open access by Scholarly Commons at Boston University School of Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Scholarly Commons at Boston University School of Law. For more information, please contact lawlessa@bu.edu.

BOSTON UNIVERSITY

PRIVACY IN PANDEMIC: LAW, TECHNOLOGY, AND PUBLIC HEALTH IN THE COVID-19 CRISIS

Tiffany C. Li[*]

ABSTRACT

The COVID-19 pandemic has caused millions of deaths and disastrous consequences around the world, with lasting repercussions for every field of law, including privacy and technology. The unique characteristics of this pandemic have precipitated an increase in use of new technologies, including remote communications platforms, healthcare robots, and medical AI. Public and private actors are using new technologies, like heat sensing, and technologically-influenced programs, like contact tracing, alike in response, leading to a rise in government and corporate surveillance in sectors like healthcare, employment, education, and commerce. Advocates have raised the alarm for privacy and civil liberties violations, but the emergency nature of the pandemic has drowned out many concerns.

This Article is the first comprehensive account of privacy impacts related to technology and public health responses to the COVID-19 crisis. Many have written on the general need for better health privacy protections, education privacy protections, consumer privacy protections, and protections against government and corporate surveillance. However, this Article is the first comprehensive article to examine these problems of privacy and technology specifically in light of the pandemic, arguing that the lens of the pandemic exposes the need for both widescale and small-scale reform of privacy law. This Article approaches these problems with a focus on technical realities and social salience, and with a critical awareness of digital and political inequities, crafting normative recommendations with these concepts in mind.

Understanding privacy in this time of pandemic is critical for law and policymaking in the near future and for the long-term goals of creating a future society that protects both civil liberties and public health. It is also important to create a contemporary scholarly understanding of privacy in pandemic at this moment in time, as a matter of historical record. By examining privacy in pandemic, in the midst of pandemic, this Article seeks to create a holistic scholarly foundation for future work on privacy, technology, public health, and legal responses to global crises.

---

[*] Clinical Assistant Visiting Professor, Boston University School of Law; Fellow, Yale Law School Information Society Project. The author thanks Tally Amir, Chinmayi Arun, Jack M. Balkin, Lindsey Barrett, Danielle Keats Citron, James Grimmelmann, Woodrow Hartzog, Stephanie Hsia, Bonnie Kaplan, Michael Karanicolas, Jisu Kim, Bonnie Kaplan, Asaf Lubin, Michael Meuer, Przemyslaw Palka, Shlomit Yanisky-Ravid, Andrew Sellars, David Seipp, Kate Silbaugh, Christina Spiesel, Rory Van Loo, Patricia Vargas, David Thaw, Laurin Weissinger, Shlomit Yanisky-Ravid, Kathy Zeiler, and the participants of the Yale Information Society Project fellows workshop, the Boston University School of Law faculty workshop, and the Intellectual Property Scholars Conference, for their helpful feedback and guidance, as well as Sasha Dudding for excellent research assistance.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

TABLE OF CONTENTS

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

INTRODUCTION

Alison Schwartz, 29 years old, a *People Magazine* staffer in New York City.

Adolph "T.J." Mendez, 44 years old, a father of six in New Braunfels, Texas.

Nashom Wooden, 50 years old, a drag queen in New York City.

Judge Kevin Thomas Duffy, 87 years old, a federal judge for the Southern District of New York.

Sarah Herbert, 5 years old, the daughter of two essential workers in Detroit, Michigan.

These[1] are just five of the hundreds of thousands of people[2] who have died of the global COVID-19 pandemic. Millions more have been infected and recovered,[3] some with lasting health ramifications and some, particularly in countries like the United States, with staggering hospital bills.[4] The pandemic has caused untold damage to people all around the world and has spurred small to drastic shifts in the use of technology across sectors. This Article explores the privacy aspect of new technologies and new technologically influenced initiatives deployed as part of the COVID-19 response by both public and private actors.

COVID-19, also known as the "novel coronavirus," or SARS-CoV-2, is a highly contagious virus that causes a range of symptoms in humans, often

---

[1] From Buzzfeed's moving collection of profiles, at *The Victims of COVID-19*, BUZZFEED (Apr. 2, 2020, 12:38 PM ET), https://www.buzzfeednews.com/article/buzzfeednews/the-victims-of-covid-19.

[2] *See Coronavirus Tracked: The Latest Figures as Countries Fight to Contain the Pandemic*, FIN. TIMES, https://www.ft.com/content/a26fbf7e-48f8-11ea-aeb3-955839e06441 (last accessed May 21, 2020).

[3] More than 13.4 million as of July 16, 2020. *See Coronavirus Tracked: The Latest Figures as Countries Fight to Contain the Pandemic*, FIN. TIMES, https://www.ft.com/content/a26fbf7e-48f8-11ea-aeb3-955839e06441 (last accessed July 16, 2020).

[4] Abigail Abrams, *America's Health System Will Likely Make the Coronavirus Outbreak Worse*, TIME (Mar. 4, 2020), https://time.com/5794672/health-insurance-deductibles-coronavirus; Abigail Abrams, *Total Cost of Her COVID-19 Treatment: $34,927.43*, TIME (Mar. 19, 2020), https://time.com/5806312/coronavirus-treatment-cost.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

primarily attacking the respiratory system.[5] There are a few unique characteristics of COVID-19 that are important to note when examining the use of technology in the public health, government, and corporate response to the virus. First, the virus is fast-moving, with global reach. Though the outbreak was first declared a Public Health Emergency by the World Health Organization on January 30, 2020,[6] the virus quickly reached most parts of the world in a manner of months. Second, the virus is deadly. As of May 2020, the virus has killed almost 300,000 worldwide,[7] including 105,000 in the United States alone, as of June 3.[8] Third, the virus is highly contagious. Early research suggests it may spread through tiny virus particles released from infected individuals, potentially transmitting through coughs, sneezes, talking, breathing[9], or potentially even through the air.[10] Fourth, the virus can be invisible. Individuals infected with the virus may take up to two weeks to develop symptoms, and many may be completely asymptomatic.

These four factors (fast-moving spread, contagiousness, deadliness, and potential for invisible, asymptomatic transmission) have led to severe measures to help stem or stop viral transmission. Social distancing[11] has become the rule for many regions, including entire nations. The concept behind social distancing is that the virus will spread more slowly if humans do not get close enough to each other to be in range of virus particles released from breath,[12] touch, and so on. To support social distancing, governments have shut down schools, businesses, retail, restaurants, and more. The shutdowns have contributed to

---

[5] Neel V. Patel, *How Does the Coronavirus Work?*, MIT TECH. REV. (Apr. 15, 2020), https://www.technologyreview.com/2020/04/15/999476/explainer-how-does-the-coronavirus-work.

[6] *Rolling Updates on Coronavirus Disease (COVID-19)*, WORLD HEALTH ORG., https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen (last updated May 19, 2020).

[7] FIN. TIMES, *supra* note 3.

[8] Joe Fox et al., *At Least 92,000 People Have Died From Coronavirus in the U.S.*, WASH. POST (June 3, 2020), https://www.washingtonpost.com/graphics/2020/national/coronavirus-us-cases-deaths/.

[9] *How COVID-19 Spreads*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/how-covid-spreads.html.

[10] Lisa Lockerd Maragakis, *Coronavirus Disease 2019 vs. the Flu*, JOHNS HOPKINS MED., https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus/coronavirus-disease-2019-vs-the-flu.

[11] Josiah Bates, *What Is 'Social Distancing?' Here's How to Best Practice It as Coronavirus Spreads*, TIME (Mar. 11, 2020), https://time.com/5800442/social-distancing-coronavirus./

[12] David Williams, *How Coronavirus Spread from One Member to 87% of the Singers at a Washington Choir Practice*, CNN (May 13, 2020), https://edition.cnn.com/2020/05/13/us/coronavirus-washington-choir-outbreak-trnd/index.html; *Loud Talking Could Leave Coronavirus in the Air for Up to 14 Minutes*, MIT TECH. REV. (May 13, 2020), https://www.technologyreview.com/2020/05/13/1001696/loud-talking-could-leave-coronavirus-in-the-air-for-up-to-14-minutes.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

mass unemployment.[13] (Over 11 million Americans lost their jobs in March 2020 alone.[14]) The U.S. Centers for Disease Control and Prevention (CDC), as well as many states, have also encouraged people to wear masks at all times when outside or near the presence of others.[15] As of May 2020, scientists expect a vaccine may not be ready until 2021.[16]

States have attempted to respond to the crisis by using technological solutions to try to stop or slow the spread of the novel coronavirus. Many of these solutions have been data-driven, with few if any guarantees for individual data privacy. These technology-influenced solutions include Bluetooth tracking, cell-phone location data tracking, various types of testing (including antigen and antibody testing), immunity passports or certification, human and digital contact tracing, and more. Public health responses have included increased use of telemedicine and telehealth (often through remote communication technologies), as well as use of medical AI and healthcare robots. Governments have used surveillance technologies, like facial recognition and remote heat sensing, as part of response efforts as well. As always, with new government surveillance comes new risks and dangers to civil liberties and privacy, particularly for marginalized populations.[17]

Corporations, too, have developed and implemented new technological programs in response to this pandemic. Consumer technologies, including remote communication technologies, have risen to the forefront. These technologies have also been used in the work setting, as many white-collar workers have moved to remote offices. All of these programs come with their own risks to security and privacy. Corporate surveillance also extends to the physical realm, as companies have instituted privacy-invasive measures like temperature checks for employees.

---

[13] Sylvan Lane, *More Than 11 Million Laid Off in March as Coronavirus Spread Through US*, HILL (May 15, 2020), https://thehill.com/policy/finance/498005-more-than-11-million-laid-off-in-march-as-coronavirus-spread-through-us.

[14] *Id.*

[15] *Recommendation Regarding the Use of Cloth Face Coverings, Especially in Areas of Significant Community-Based Transmission*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/cloth-face-cover.html.

[16] Quentin Fotrell, *'The 1918 Spanish Flu's Second Wave Was Even More Devastating': Americans Brace for Another Coronavirus Outbreak in the Fall*, MARKETWATCH (May 21, 2020), https://www.marketwatch.com/story/we-will-not-have-a-vaccine-by-next-winter-what-happens-when-coronavirus-returns-2020-04-22.

[17] DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); Mary A. Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 441 (2017); Scott Skinner-Thompson, *Performative Privacy*, 50 DAVIS L. REV.1673 (2017); Scott Skinner-Thompson, *Privacy's Double Standards*, 93 WASH. REV 2051 (2018) [hereinafter Skinner-Thompson, *Privacy's Double Standards*])

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Outside of government public health response and corporate employee surveillance, individuals have seen changes in the use of technologies and privacy protections in other sectors as well. Many corporate surveillance technologies are also being used in the education sector, putting the privacy of students and educators at risk. At the same time, the social distancing measures necessary for life in a pandemic have led to an increase in the use of remote communication technologies in private life, changing the way individuals experience technology in the workplace, in education, and in social lives.

This Article examines privacy aspects of new technologies and technologically-influenced public health responses that have risen to the forefront as a result of the pandemic. Understanding privacy in this time of pandemic is critical, both for our near future and for the long-term goals of creating a future society that protects both civil liberties and public health. Certainly, with the benefit of hindsight, future scholars will likely find that many of the technological solutions proposed and implemented now were actually unhelpful or perhaps even harmful. However, examining how privacy was considered and understood during the pandemic will aid future scholarship and support the efforts of others tasked with shaping laws that deal with privacy in future global crises, in addition to adding to the longitudinal study of our society's ever-changing relationship with data and technology over time.

The Article first looks at public-health programs that have developed as part of pandemic response. These programs include COVID-19 testing programs, contact tracing programs, immunity passports, and novel uses of technology in medicine and healthcare, including medical AI and healthcare robots. Next, the Article explores the privacy impacts of new technologies through a variety of sectors: government surveillance; employee surveillance; educational privacy; and consumer privacy. Finally, the Article offers normative recommendations for protecting privacy while also supporting public health.

While a growing body of scholarship is rapidly developing on legal issues related to the COVID-19 pandemic[18], this Article provides the first comprehensive analysis of privacy, technology, and public health responses across sectors. Furthermore, this Article is unique in explaining the technical and scientific components of each of these privacy-affective technological solutions, as well as focusing on the societal changes that have pushed the use of these technologies and have come about as a result of these technological changes. Most of the technologies being deployed as COVID-19 responses are not new. As Jack M. Balkin has opined, the novelty of new technologies is not

[18] See, e.g., this in-progress special issue of the Journal of Law and Biosciences: https://blog.petrieflom.law.harvard.edu/2020/06/09/pandemic-issue-journal-of-law-and-the-biosciences/

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

what matters for understanding how the law should regulate. Rather, it is what has changed in society that has driven the rise in certain technologies that we should seek to understand. In creating new laws for new technologies (or new crises), we should look to salience, not novelty.[19]

Finally, this article is unique in shedding light on critical dimensions of privacy in times of pandemic, particularly impacts on marginalized groups, including intersectional analysis of disparate harms, reflecting on Kimberlé Crenshaw's groundbreaking work on understanding the intersection of race, gender, and other identities in law, politics, and theory.[20] Understanding the impact race, gender, and other dimensions have on public health, privacy, and technology are critical, as the pandemic has highlighted inequalities throughout society.

Much further study is needed on this subject, including empirical work on privacy practices and responses, as well as research on disparate impact, and comparative research on the vastly different privacy-related programs that nations and regions have developed—influenced in no small part, to be sure, by their unique legal and regulatory regimes. This Article focuses primarily on U.S. privacy law, as well as privacy-related developments in the United States. The Article does not claim to provide an exhaustive study of all potential privacy implications of all pandemic-related interventions, but rather serves to lay the groundwork for future scholarship on these issues.

I. PUBLIC HEALTH AND PRIVACY IN PANDEMIC

There exists a long literature in bioethics and health law on concepts of privacy and individual rights in healthcare, from the concept of informed consent (far beyond the norms of notice and consent in privacy theory)[21] to questions of ethics in medical research and medical practice. Under the American sector-specific privacy law regime,[22] a smattering of laws governs

---

[19] Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 1-3 (2004).)

[20] KIMBERLÉ CRENSHAW, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 U. CHI. L.F. 139.

[21] Charlotte Tschider, *The Consent Myth: Improving Choice for Patients of the Future*, 96 WASH. U. L. REV. 1505 (2018).

[22] Unlike in some other nations, the United States lacks omnibus privacy regulation. Instead, privacy law is governed by an amalgamation of different laws and regulations for specific sectors, including particular types of data, particular types of data subjects, and particular industries. Constitutional privacy rights also come not from a clear constitutional provision, unlike in other nations, but from a "penumbra" of privacy rights. *See* Griswold v. Connecticut, 381 U.S. 479 (1965).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

health privacy and health technology, including HIPAA[23] (and the Privacy Rule and HITECH[24]), GINA,[25] FTC consumer protection law,[26] and state privacy laws. Additionally, scholars like Khiara Bridges have explored privacy in healthcare and the degrees to which different people are afforded different privacy protections based on race, income, gender, and more.[27]

This section examines public-health responses to the COVID-19 pandemic, namely: testing, immunity passports, telehealth, medical AI, and healthcare robots. While many of the technologies used for public-health pandemic response are not new,[28] the specific pressures of the COVID-19 pandemic create a unique lens through which to examine the use of technology for public health response.

A. COVID-19 Testing

Since the beginning of the pandemic, states have raced to increase their testing capabilities, in the hopes of stopping or slowing the spread of the virus.[29] Testing of any kind generates data, some of it potentially identifiable. Different public and private testing bodies have tackled testing—including public health agencies, private clinics, employers, and education institutions. Some have argued that there may be a moral duty for individuals to donate data for public health purposes in this time.[30] The rapidly increased scale of testing around the world creates an increase in potential harms related to data collection, use, and transfer. To understand the privacy dimensions of viral testing, it is first necessary to establish a baseline understanding of the tests and the parties involved in testing, before turning to privacy implications.

---

[23] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 136.

[24] 42 U.S.C. § 201 (2018).

[25] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881.

[26] CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

[27] KHIARA BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2019).

[28] Nicolas P. Terry, *Information Technology's Failure to Disrupt Health Care*, 13 NEV. NEV.L.J. 722, 723-24 (2013).

[29] Umair Irfan, *The Case for Ending the Covid-19 Pandemic with Mass Testing*, VOX (Apr. 13, 2020), https://www.vox.com/2020/4/13/21215133/coronavirus-testing-covid-19-tests-screening.

[30] Brent Mittelstadt et al., *Is There a Duty to Participate in Digital Epidemiology?*, LIFE SCI., SOC'Y & POL'Y (May 9, 2018), https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-018-0074-1.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

1. Taxonomy of COVID-19 Tests

There are three types of COVID-19 testing that have come to the forefront in pandemic response: polymerase chain reaction tests (PCR), antigen testing, and antibody tests.[31] Each of these forms of testing produce biological samples—primarily mucus or blood.

PCR tests are the most common and accurate tests for determining if a person has an active COVID-19 infection.[32] These tests are performed by a healthcare provider using a long thin swab to collect a mucus sample from an individual's throat or nose.[33] The sample is then sent to a lab (external or in-house, if the clinic or hospital has facilities) to determine if the sample contains COVID-19 genetic material—a process that may take a number of days to yield results.[34] The transport between testing location and lab may take up to twenty-four hours, and the test itself may take six hours to complete (though processing time varies by lab).[35]

Antigen tests (or rapid diagnostic tests) detect the presence of antigens (viral proteins) of the COVID-19 virus. These tests are significantly faster than PCR tests, producing results in approximately fifteen minutes, according to the CDC[36] (thirty minutes according to the WHO[37]), and are relatively simple to perform.[38] Dr. Deborah Birx, the White House coronavirus response

---

[31] Overview of Testing for SARS-CoV-2, Center for Disease Control (July 17, 2020), https://www.cdc.gov/coronavirus/2019-ncov/hcp/testing-overview.html, (last accessed July 24, 2020); *Coronavirus Testing Basics*, U.S. FOOD AND DRUG ADMINISTRATION (last accessed July 24, 2020), https://www.fda.gov/consumers/consumer-updates/coronavirus-testing-basics ; (Eric Levenson & Arman Azad, *What to Know About the Three Main Types of Coronavirus Tests*, CNN (Apr. 29, 2020), https://www.cnn.com/2020/04/28/us/coronavirus-testing-pcr-antigen-antibody/index.html.

[32] *Id.*

[33] A. Pawlowski, *Coronavirus Test: What Is it Like to Get the Nasal Swab for Detecting COVID-19?*, TODAY (Mar. 18, 2020), https://www.today.com/health/coronavirus-test-what-it-get-nasal-swab-detecting-covid-19-t176271.

[34] Eric Levenson & Arman Azad, *What to Know About the Three Main Types of Coronavirus Tests*, CNN (Apr. 29, 2020),
https://www.cnn.com/2020/04/28/us/coronavirus-testing-pcr-antigen-antibody/index.html

[35] Julie Appleby, *Why It Takes So Long To Get Most COVID-19 Test Results*, NPR (Mar. 28, 2020), https://www.npr.org/sections/health-shots/2020/03/28/822869504/why-it-takes-so-long-to-get-most-covid-19-test-results.

[36] *Rapid Influenza Diagnostic Tests*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/flu/professionals/diagnosis/clinician_guidance_ridt.htm.

[37] *Advice on the Use of Point-of-Care Immunodiagnostic Tests for COVID-19*, WORLD HEALTH ORG. (Apr. 8, 2020), https://www.who.int/news-room/commentaries/detail/advice-on-the-use-of-point-of-care-immunodiagnostic-tests-for-covid-19.

[38] *Rapid Influenza Diagnostic Tests*, CTRS. FOR DISEASE CONTROL & PREVENTION,

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

coordinator, said in April that antigen tests may be the "breakthrough" needed to test large numbers of people in the United States, given that antigen tests are simpler and faster than PCR tests.[39] However, accurate antigen tests can be difficult to produce and may be more likely to miss active infection; indeed, the World Health Organization has cautioned against their use in response to the COVID-19 pandemic due to the lack of accuracy and limited data available, as of April 2020.[40]

Antibody tests (or serological tests) "measure the amount of antibodies or proteins present in the blood when the body is responding to a specific infection, like COVID-19."[41] Antibody tests can determine whether a person has previously been exposed to a particular pathogen,[42] by detecting whether the person has developed antibodies in their immune system that would suggest a prior immune response to the novel coronavirus in the body.[43] (However, antibody tests cannot differentiate between patients with active and past infections.[44]) Antibody tests can be performed by collecting blood samples from individuals. In April 2020, Germany began conducting Europe's first nationwide COVID-19 antibody testing program.[45] The U.S. National Institutes of Health (NIH) also embarked on a program to test 10,000 U.S. volunteers for antibodies.[46]

---

https://www.cdc.gov/flu/professionals/diagnosis/clinician_guidance_ridt.htm.

[39] Arman Arzad, *Antigen Tests: The Coronavirus 'Breakthrough' That a Top White House Official Says We Need*, CNN (Apr. 27, 2020), https://www.cnn.com/2020/04/27/health/antigen-tests-coronavirus-breakthrough/index.html.

[40] *Advice on the Use of Point-of-Care Immunodiagnostic Tests for COVID-19*, WORLD HEALTH ORG. (Apr. 8, 2020), https://www.who.int/news-room/commentaries/detail/advice-on-the-use-of-point-of-care-immunodiagnostic-tests-for-covid-19.

[41] Press Release, Stephen M. Hahn, Comm'r of Food & Drugs, Food & Drug Admin., Coronavirus (COVID-19) Update: Serological Tests (Apr. 7, 2020), https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-serological-tests.

[42] https://www.centerforhealthsecurity.org/resources/COVID-19/COVID-19-fact-sheets/200228-Serology-testing-COVID.pdf.

[43] Eric Levenson & Arman Azad, *What to Know About the Three Main Types of Coronavirus Tests*, CNN (Apr. 29, 2020), https://www.cnn.com/2020/04/28/us/coronavirus-testing-pcr-antigen-antibody/index.html.

[44] Gagan Mathur and Sweta Matur, *Antibody Testing for Covid-19: Can It Be Used As a Screening Tool in Areas with Low Prevalence?*, 154 AMERICAN JOURNAL OF CLINICAL PATHOLOGY 1 (May 15, 2020).

[45] Rob Schmitz, *Germany Is Conducting Nationwide COVID-19 Antibody Testing*, NPR (Apr. 21, 2020), https://www.npr.org/sections/coronavirus-live-updates/2020/04/21/839594202/germany-is-conducting-nationwide-covid-19-antibody-testing.

[46] Apoorva Mandavilli & Katie Thomas, *Will an Antibody Test Allow Us to Go Back to School or Work?*, N.Y. TIMES (Apr. 10, 2020), https://www.nytimes.com/2020/04/10/health/coronavirus-antibody-test.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

At this time, it is still uncertain how strong immunity might be or how long it might last.[47] There have been cases of people testing positive twice (likely due to having higher levels of antibodies when first tested and lower level of antibodies when tested later), seemingly not developing immunity to the virus.[48] Antibody tests may also have a problem with accuracy,[49] especially because the Food and Drug Administration (FDA) has issued a policy allowing developers of some serological tests to bring to market their tests without prior FDA review.[50] In April 2020, the WHO recommended against the use of antibody tests as diagnostics for patient care, but encouraged their use for "disease surveillance and epidemiological research."[51]

Some have suggested the use of antibody tests to "re-open" society[52] as the

---

[47] Eric Levenson & Arman Azad, *What to Know About the Three Main Types of Coronavirus Tests*, CNN (Apr. 29, 2020), https://www.cnn.com/2020/04/28/us/coronavirus-testing-pcr-antigen-antibody/index.html; Apoorva Mandavilli & Katie Thomas, *Will an Antibody Test Allow Us to Go Back to School or Work?*, N.Y. TIMES (Apr. 10, 2020),; https://www.nytimes.com/2020/04/10/health/coronavirus-antibody-test.html.

[48]John Bacon, Can you get infected with COVID-19 twice? Experts say possibility is 'certainly real', USA TODAY (July 16, 2020, 3:17 PM ET), https://www.usatoday.com/story/news/health/2020/07/16/covid-19-can-you-get-infected-twice-herd-immunity/5429012002/

[49] Gagan Mathur and Sweta Matur, *Antibody Testing for Covid-19: Can It Be Used As a Screening Tool in Areas with Low Prevalence?*, 154 AMERICAN JOURNAL OF CLINICAL PATHOLOGY 1 (May 15, 2020); Apoorva Mandavilli & Katie Thomas, *Will an Antibody Test Allow Us to Go Back to School or Work?*, N.Y. TIMES (Apr. 10, 2020), https://www.nytimes.com/2020/04/10/health/coronavirus-antibody-test.html.

[50] Press Release, Stephen M. Hahn, Comm'r of Food & Drugs, Food & Drug Admin., Coronavirus (COVID-19) Update: Serological Tests, https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-serological-tests.

[51] *Advice on the Use of Point-of-Care Immunodiagnostic Tests for COVID-19*, WORLD HEALTH ORG. (Apr. 8, 2020), https://www.who.int/news-room/commentaries/detail/advice-on-the-use-of-point-of-care-immunodiagnostic-tests-for-covid-19.

[52] *See, e.g.*, Aaron Edlin & Bryce Nesbitt, *The 'Certified Recovered' from Covid-19 Could Lead the Economic Recovery*, STAT (Apr. 6. 2020), https://www.statnews.com/2020/04/06/the-certified-recovered-from-covid-19-could-lead-the-economic-recovery; Opinion, Ezekiel J. Emanuel, *We Can Safely Restart the Economy in June. Here's How.*, N.Y. TIMES (Mar. 28, 2020), https://www.nytimes.com/2020/03/28/opinion/coronavirus-economy.html; Veronika Hackenbroch, *Große Antikörperstudie Soll Immunität Der Deutschen Gegen Covid-19 Feststellen*, DER SPIEGEL (Mar. 27, 2020), https://www.spiegel.de/wissenschaft/medizin/coronavirus-grosse-antikoerper-studie-soll-immunitaet-der-deutschen-feststellen-a-c8c64a33-5c0f-4630-bd73-48c17c1bad23; Jason Horowitz, *In Italy, Going Back to Work May Depend on Having the Right Antibodie*s, N.Y. TIMES (Apr. 4, 2020), https://www.nytimes.com/2020/04/04/world/europe/italy-coronavirus-antibodies.html; Carolyn Y. Johnson, *Testing Coronavirus Survivors' Blood Could Help Reopen U.S.*, WASH. POST (Mar. 31, 2020, 12:35 PM EDT), https://www.washingtonpost.com/health/2020/03/31/coronavirus-serology-blood-tests.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

pandemic slows. These tests could be used to determine or prove immunity to the virus, a form of validation that could then be used for "immunity passports" that could allow individuals to do certain types of work, travel, or do other higher risk activities.[53] These immunity passports (and related proposals) come with a host of privacy, algorithmic accountability, and digital inequity issues,[54] as discussed later in this paper. However, it is uncertain if antibody tests can be used as an effective screening tool to allow re-opening of schools or businesses in areas with high prevalence of COVID-19[55], regardless of how immunity passport proposals develop.

2. Taxonomy of Testing Actors

When discussing privacy, it is always critical to determine which actors are involved in collecting, using, sharing, and storing data. As the pandemic progresses, a number of agents have become involved in testing. The public-private divide may be a less useful distinction here, as many testing programs have developed as public-private partnerships (which itself raises a number of issues in terms of regulatory oversight). For example, the controversial data analytics company Palantir Technologies partnered with the Department of Health and Human Services and the Center for Disease Control, with the technology company offering "data tools … to 'clean' and 'harmonize' the information flowing in from local hospitals, states and other sources related to the virus."[56]

Some nations have implemented national testing campaigns for public health. For example, in April 2020, Germany began conducting Europe's first

---

See, e.g., https://www.washingtonpost.com/health/2020/03/31/coronavirus-serology-blood-tests/; https://www.nytimes.com/2020/04/04/world/europe/italy-coronavirus-antibodies.html; https://www.statnews.com/2020/04/06/the-certified-recovered-from-covid-19-could-lead-the-economic-recovery/; https://www.spiegel.de/wissenschaft/medizin/coronavirus-grosse-antikoerper-studie-soll-immunitaet-der-deutschen-feststellen-a-c8c64a33-5c0f-4630-bd73-48c17c1bad23; https://www.nytimes.com/2020/03/28/opinion/coronavirus-economy.html

[53] Lydia Smith, *Germany to Introduce Coronavirus 'Immunity Certificates' for Recovered Public*, NEWSWEEK (Mar. 30, 2020), https://www.newsweek.com/germany-antibodies-tests-general-public-immunity-certificates-1494934.

[54] Henry T. Greely, *Covid-19 'Immunity Certificates': Practical and Ethical Conundrums*, STAT (Apr. 10, 2020), https://www.statnews.com/2020/04/10/immunity-certificates-covid-19-practical-ethical-conundrums.

[55] Gagan Mathur and Sweta Matur, *Antibody Testing for Covid-19: Can It Be Used As a Screening Tool in Areas with Low Prevalence?*, 154 AMERICAN JOURNAL OF CLINICAL PATHOLOGY 1 (May 15, 2020);

[56] Jackson Barnett, *Inside Palantir's work with the CDC, HHS to synthesize COVID-19 data*, FEDSCOOP (April 2, 2020), https://www.fedscoop.com/palantir-covid-19-coronavirus-data-cdc-hhs/.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

nationwide COVID-19 antibody testing program.[57] The U.S. NIH also embarked on a much more limited program to test 10,000 U.S. volunteers for antibodies.[58] Across the United States, states, counties, and cities have developed testing campaigns, some as public programs and some as public-private partnerships.[59]

In the absence of, or perhaps in addition to, federally-driven nationwide testing in the U.S., this mishmash network of testing programs has created a fairly large cast of characters—parties that could be considered data controllers or processors[60] for data generated from COVID-19 related testing. (While the U.S. does not generally use the data controller vs. processor framework[61] for privacy regulation, it can be a useful metric for understanding the roles of different actors in the data lifecycle of COVID-19 testing.)

The parties involved at the primary point of collection include private companies (particularly in technology and healthcare industries), universities and research centers, hospitals and healthcare providers, governments, and—in the case of distributed or open data projects—potentially the public. Many of these would fulfill a data controller-like role. U.S. Federal Trade Commission (FTC) privacy regulation would also apply to many testing actors collecting data or performing testing.[62]

Third parties that may obtain or have interest in COVID-19 testing data include relevant health and technology companies and organizations, as well as (potentially) downstream commercial actors, including data brokers and unrelated companies that may wish to use the data for other purposes (e.g.,

---

[57] Rob Schmitz, *Germany Is Conducting Nationwide COVID-19 Antibody Testing*, NPR (Apr. 21, 2020), https://www.npr.org/sections/coronavirus-live-updates/2020/04/21/839594202/germany-is-conducting-nationwide-covid-19-antibody-testing.

[58] Apoorva Mandavilli & Katie Thomas, *Will an Antibody Test Allow Us to Go Back to School or Work?*, N.Y. TIMES (Apr. 10, 2020), https://www.nytimes.com/2020/04/10/health/coronavirus-antibody-test.html.

[59] *See, e.g.,* https://www.hhs.gov/about/news/2020/06/30/hhs-extends-covid-19-testing-public-private-partnership.html

[60] In E.U. data protection law, most notably in the General Data Protection Regulation, a data controller "determines the purposes for which and the means by which personal data is processed," while a data processor processes the data on behalf of a controller. See *https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en*

[61] Jones, Meg and Kaminski, Margot E., An American's Guide to the GDPR (June 5, 2020). Denver Law Review, Vol. 98, No. 1, 2020.

[62] For example, private companies conducting testing would likely fall under FTC jurisdiction regarding unfair and misleading practices involved with testing and promises made to consumers.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

marketing health products). Additionally, government actors may have or may obtain access to COVID-19 testing data—both for direct COVID-19 response purposes as well as potentially other purposes, including government surveillance and law enforcement. Finally, no system is ever fully secure, so with any collection of COVID-19 testing data, there will always be the threat of bad actors accessing or obtaining data. These bad actors could potentially include foreign state actors, leading to national security concerns.

It is useful to understand which actors are involved throughout the data lifecycle of data obtained from or generated by COVID-19 testing, particularly for regulators and policymakers who wish to govern these practices and actors, as well as for individuals to later seek legal or other recourse.

3. Taxonomy of COVID Data

There are many types of data relevant to a privacy analysis of the COVID-19 testing process. It is beyond the scope of this paper (and not useful, perhaps) to attempt to define every type of data in every possible taxonomy. However, here are a few important categories of data to consider when thinking about privacy and COVID-19 testing.

COVID-19 testing, be it polymerase chain reaction tests (PCR), antigen testing, or antibody tests,[63] involves collecting biological samples—primarily mucus or blood. These samples are then analyzed to determine if a person has been exposed to the virus or has a current viral infection. Different forms of data are generated by COVID-19 testing. These include the biological samples or specimens, of course, but also more data collected and generated throughout the process.

Consider, for example, the health data connected to the patient that is collected when individuals enter the primary point of collection (e.g., testing center, hospital, research center). If a patient signs in at the front desk of a hospital, that is data that could potentially be linked to data generated by the person's testing process. Data collectors (e.g., hospitals and researchers) may ask additional questions (e.g., asking for symptoms) during the testing process, and individuals may offer additional data (e.g., demographic data). Other biological samples may also be taken, for analysis of other factors that are not directly related to COVID-19 viral presence. The analysis phase (where biological samples are analyzed by labs) can produce more data, including but not limited

[63] Eric Levenson & Arman Azad, *What to Know About the Three Main Types of Coronavirus Tests*, CNN (Apr. 29, 2020), https://www.cnn.com/2020/04/28/us/coronavirus-testing-pcr-antigen-antibody/index.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

to data determining COVID-19 exposure.

A non-exhaustive list of types of data that may be generated throughout the COVID-19 testing lifecycle include:

- Biological samples (including samples used for COVID-19 detection as well as other samples)
- Genetic data (obtained from biological samples or from other sources)[64]
- Health data (obtained throughout the process)
- Other personal data, broadly defined[65]

Health data is a broad category, and different laws define categories of data that merit special protection. For example, HIPAA protects "protected health information" (PHI), which is defined as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."[66] HIPAA does not cover the protection of health-related information that is not transmitted through the statutorily defined means or the protection of health information that may be arguably non-identifiable and does not protect other categories of information related to health. For example, Mason Marks has also identified "emerging medical data," data from social media and other sources, that could effectively provide the same insights as traditional health data.[67] This is a category of data that is not covered by existing U.S. laws on health privacy.

Genetic information is defined in (among other places) the Genetic Information Nondiscrimination Act (GINA), one of the leading genetic data laws in the United States. GINA defines genetic information, as, with respect to any individual, "information about (i) such individual's' genetic tests, (ii) the genetic tests of family members of such individual, and (iii) the manifestation of a disease or disorder in family members of such individual."[68] GINA defines a genetic test as a "an analysis of human DNA, RNA, chromosomes, proteins, or

---

[64] For example, 23andMe's study relied on its existing databank of genetic information collected previously. *See* Megan Molteni, *Why Does Covid-19 Make Some People So Sick? Ask Their DNA*, WIRED (Apr. 7, 2020), https://www.wired.com/story/why-does-covid-19-make-some-people-so-sick-ask-their-dna.

[65] The distinction between personally identifiable data and data deemed to not be personally identifiable has not been found to be useful in practice, as many forms of data can be re-identifiable. *See* Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLAL.REV.1701 (2010).

But cf. Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1 (2011).

[66] 45 CFR § 160.103 (2019).

[67] Mason Marks, *Emergent Medical Data: Health Information Inferred by Artificial Intelligence*, 11 U.C. IRVINE L. REV. (forthcoming (2021),).https://ssrn.com/abstract=3554118.

[68] 42 U.S.C.USCS § 300gg–91(d)(16) (2018).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

metabolites, that detects genotypes, mutations, or chromosomal changes," excluding (i) analysis of proteins or metabolites that does not detect genotypes, mutations, or chromosomal changes; or (ii) an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a healthcare professional with appropriate training and expertise in the field of medicine involved.[69]

HIPAA also includes genetic information as potentially falling under the umbrella of PHI. The Privacy Rule "(1) revise[d] the definition of "health information" to make clear that the term includes "genetic information;" and (2) add[ed] definitions for the GINA-related terms of "family member," "genetic information," "genetic services," "genetic test," and "manifestation or manifested;"[70] HIPAA's genetic information definition includes the categories of information covered under the definition of genetic information under GINA as well as "any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual."[71]

Some of the data collected or processed in the testing data lifecycle might qualify as genetic data—or might deserve the special protections afforded to genetic data. Genetic data is particularly important to protect due to the importance genes have to our conceptions of identity and self. Alondra Nelson has described the "special status afforded to DNA as the final arbiter of truth of identity"[72] and has called DNA "the ultimate big data."[73] The unique sensitivity of genetic data is also important to keep in mind in the debate over immunity passports based on antibody tests.

Additionally, health privacy laws often fail to recognize non-health information that is also at risk with health information disclosures. Other personal data may include demographic data, data on social or personal habits that may not be health-related in nature, as well as data that could appear on first glance to be unrelated to the COVID-19 testing lifecycle. Disclosure of non-health data can also lead to privacy harms. For example, one coronavirus outbreak in South Korea was traced to a nightlife area that included many clubs popular with the local LGBTQ community. In disclosing the source of the

---

[69] 42 U.S.C.USCS § 300gg–91 (d)(17) (2018).

[70] HIPAA Administrative Simplification: Standards for Privacy of Individually Identifiable Health Information, 74 Fed. Red.FR 51698 (Oct. 7, 2009).

[71] 45 C.F.R. § 160.103 (2019).

[72] ALONDRA NELSON, THE SOCIAL LIFE OF DNA: RACE, REPARATIONS, AND RECONCILIATION AFTER THE GENOME 4 (2016).

[73] *Id.*

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

outbreak, health authorities potentially jeopardized the safety of the LGBTQ people who had frequented the district in secret.[74]

It is important to understand which types of data are being collected and processed throughout the COVID-19 testing lifecycle, because different types of data sometimes need different legal and regulatory protections. For example, health data and genetic data merit special protection under different laws and regulations in the U.S. sector-specific privacy regime. Personal data not directly related to health or genetics also merits protection, particularly personal data that is easily identifiable. Biological samples or specimens may need different security protections than digital data. Other data that does not fall easily into any of the above categories should not be excluded from protection either, particularly given the ability for downstream data aggregators to amass large data sets that could then lead to reidentification.

4. Understanding the COVID-19 Testing Data Lifecycle

To understand the data flow and lifecycle of data generated from testing, start at the beginning.

First, a person gives a sample (biological or data, as in survey responses) to a primary data collector. This first phase—the primary point of collection—may involve multiple primary data collectors. For example, a person may go to a drive-through testing center, jointly managed by the state government, a local hospital, and private testing companies. Thus, at the primary point of collection, a number of parties may have control over the data and qualify as data controllers as traditionally understood.

The primary data collection from COVID-19 testing takes place at a number of points of collection: traditional healthcare settings (e.g., hospitals, primary care practices); new testing facilities (e.g., COVID-19 specific drive-through testing centers)[75]; public and private research settings (e.g., 23andMe's genetic study[76] and UCSF's citizen science epidemiology app[77]); and distributed or open

---

[74] https://time.com/5836699/south-korea-coronavirus-lgbtq-itaewon/; https://www.wsj.com/articles/south-koreas-coronavirus-efforts-spark-privacy-concerns-in-gay-community-11589306659

[75] Press Release, Governor Cuomo Opens the State's First Drive-through COVID-19 Mobile Testing Center in New Rochelle, Gov. Andrew M. Cuomo (Mar. 13, 2020), https://www.governor.ny.gov/news/governor-cuomo-opens-states-first-drive-through-covid-19-mobile-testing-center-new-rochelle-0.

[76] Megan Molteni, *Why Does Covid-19 Make Some People So Sick? Ask Their DNA*, WIRED (Apr. 7, 2020), https://www.wired.com/story/why-does-covid-19-make-some-people-so-sick-ask-their-dna.

[77] Jeff Norris, *New COVID-19 'Citizen Science' Initiative Lets Any Adult with a Smartphone*

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

networks.[78] In early May 2020, the FDA approved the first at-home saliva test for COVID-19,[79] following its emergency authorization for the first at-home nasal swab testing kit in April 2020.[80] For this emergency authorization, the FDA relied[81] on the public health emergency powers given to it under Section 564(a) of the Federal Food, Drug, and Cosmetic Act.[82] Thus, an individual's home setting may also be a location for primary collection of samples and data, and an individual (or friends or family) may be the primary collector of the sample.

The second phase of the data lifecycle for testing data is analysis of the sample. In this phase, the primary data collector either (1) conducts analysis itself; or (2) transfers the data for analysis by another party. For example, a drive-through testing center could transfer the biological samples to a lab for analysis. Alternatively, a hospital may have the resources to both collect a sample and analyze it in an in-house lab. An individual using a home testing kit could send in the kit to the lab. In this analysis phase of the COVID-19 data lifecycle, data may be accessed, stored, and shared by parties that may be data processors or may be both processor and controller.[83]

The first two phases of the COVID-19 testing data lifecycle are relatively clear. However, as with all data collection, it is difficult to fully predict the flow of data the further downstream you get from the primary point of collection. Results of tests may be transferred to other entities, either by the individual who was tested, or by any of the testing data processors, data collectors, or data

---

Help to Fight Coronavirus, U.C. SAN FRANCISCO (Mar. 30, 2020), https://www.ucsf.edu/news/2020/03/417026/new-covid-19-citizen-science-initiative-lets-any-adult-smartphone-help-fight.

[78] *Science Friday: Citizen Scientists: Submit Your COVID-19 Symptoms (Or Lack Of Them)*, WNYC (Mar. 27, 2020), https://www.sciencefriday.com/segments/citizen-science-covid-19; Paul Sisson, *Door Knobs, Trash Cans, Gas Pumps: Citizen Scientists Search for Coronavirus on Everyday Surfaces*, SAN DIEGO UNION TRIB. (May 14, 2020); https://www.sandiegouniontribune.com/news/health/story/2020-05-14/door-knobs-trash-cans-gas-pumps-citizen-scientists-enlisted-to-help-find-coronavirus-on-everyday-surfaces.

[79] Letter from Denise M. Hinton, Chief Scientist, Food & Drug Admin., to Christian Bixby, Assistant Dir., Research & Clinical Lab Servs., Rutgers Clinical Genomics Lab., Rutgers Univ. (May 7, 2020), https://www.fda.gov/media/137773/download; Sheila Kaplan & Natasha Singer, *F.D.A. Clears First Home Saliva Test for Coronavirus*, N.Y. TIMES (May 8, 2020), https://www.nytimes.com/2020/05/08/health/fda-coronavirus-spit-test.html.

[80] Katie Thomas & Natasha Singer, *F.D.A. Authorizes First In-Home Test for Coronavirus*, N.Y. TIMES (Apr. 21, 2020), https://www.nytimes.com/2020/04/21/health/fda-in-home-test-coronavirus.html.

[81] Letter from Denise M. Hinton, Chief Scientist, Food & Drug Admin. to Christian Bixby, Assistant Dir., Research & Clinical Lab Servs., Rutgers Clinical Genomics Lab., Rutgers Univ. (May 7, 2020), https://www.fda.gov/media/137773/download.

[82] 21 U.S.C. § 360bbb–3 (2018).

[83] Jones, Meg and Kaminski, Margot E., An American's Guide to the GDPR (June 5, 2020). Denver Law Review, Vol. 98, No. 1, 2020.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

controllers. The transfer may be done intentionally or unintentionally, for the purposes specified at point of collection or not. This may include releasing information to the public about people who may have been infected with the virus. For example, places of business may post notices if an employee tests positive, or local governments may post information about large events an infected person had visited. Data from various sources may eventually find its way to data aggregators, who may repackage the data with data from many sources, increasing the chances of reidentification and potential harm (including algorithmic harms) to data subjects.

Understanding the lifecycle of testing data is key for identifying the points at which regulation can have the greatest impact on protecting privacy.

5. Legal and Regulatory Interventions to Protect Testing Data Privacy

It is helpful to break down the legal and regulatory landscape by identifying at which points law might apply to protect privacy rights. This includes identifying which actors the law can regulate, as well as identifying which actions or settings the law can govern. While testing for disease is not new, the scale at which testing has progressed is new and arguably not contemplated in current privacy laws.

The American privacy regime lacks a comprehensive federal privacy regulation. However, the United States has a number of sector-specific privacy laws and regulations that would likely pertain to the type of testing done for COVID-19 response.

a. Regulating by Data Type

For the types of data gathered in testing, we can look to regulations and legal protections for health data, genetic data, and other data. There are a number of laws that create special protections for health information as well as genetic information (sometimes separately, sometimes categorized as health information).

The United States also has federal laws specifically protecting privacy for health information. HIPAA,[84] the HIPAA Privacy Rule codified in 2002,[85] and

[84] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat 1936 (1996).)

[85] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. §§160, 164 (2019)); *s*). *ee also* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (codified at 45 C.F.R. §§ 160, 162, 164 (2019));),HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390 (Feb. 16, 2006) (codified at 45 C.F.R. §§ 160, 164 (2019));). Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Heath Information

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

2009's HITECH (the Health Information Technology for Economic and Clinical Health Act, particularly important for tightening legal protections in HIPAA) award special protection to personal health information. HIPAA includes protections for electronic health information transmission, primarily through the Privacy Rule and the Security Rule found in Section II.

However, these protections are quite limited. First, the regulations only apply to "covered entities" and, to some extent, their "business associates." Covered entities often include hospitals and clinics, but do not include many other actors that might be data collectors in the COVID-19 testing process. Under HIPAA, the covered entities that must comply with HIPAA obligations include health care providers (e.g., doctors, clinics, psychologists, dentists, nursing homes) that transmit information in an electronic form in connection with a transaction for which HIPAA applies. Covered entities also include health care clearinghouses (entities that process health information from other entities) as well as health plans (e.g., health insurance companies, HMOs, company health plans). For example, if there are no covered entities involved in the data lifecycle of a particular testing program, actors like university research centers would likely be able to evade HIPAA regulation, as would private companies like 23andMe. This could easily happen, if non-covered entities engage in their own testing or data collection programs. These programs then would lack the protections awarded under a HIPAA-compliant regime.

Second, HIPAA only awards protections to data that is electronically transmitted from a covered entity. While the regulation includes security requirements (under the Security Rule), there is little protection against more distributed downstream uses of data, which would be difficult to enforce. For example, the law does not include enforcement mechanisms for improper transfer of data by a third party who receives information from a business associate of a covered entity. Finally, HIPAA is a consent-based regime. That is, under HIPAA, covered entities and their business associates are free to collect, use, and share data as long as individuals provide their consent to such practices. Many scholars have noted the flaws of notice and consent regimes,[86] and these flaws are readily apparent in the COVID-19 testing context. Furthermore, the Department of Health and Human Services (DHHS) already relaxed some of these HIPAA restrictions, given the medical needs raised by the pandemic.[87] It

---

Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. §§ 160, 164 (2019)).).

[86] *See, e.g.*, Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. HARV.L. REV. REV.1880, 1894 (2013); Charlotte Tschider, *The Consent Myth: Improving Choice for Patients of the Future*, 96 WASH. U. L. REV. 1505 (2018)..

[87] *COVID-19 & HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public*

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

is likely that greater regulatory leniency may come as the pandemic progresses.

In the United States, genetic data is given increased protections through genetic nondiscrimination laws like GINA and some state laws that protect information including genetic information. GINA, however, is quite limited, only regulating health plans and employers and only in the context of discrimination. Many have argued for expansion of legal protection for genetic information, potentially including new laws on genetic privacy[88] and genetic discrimination.[89] For example, Ifeoma Ajunwa has called for the creation of a new tort of genetic information disclosure as well as more rigorous informed consent guidelines for genetic testing.[90] Ajunwa has also called for strengthening GINA to add a disparate impact cause of action,[91] addressing gaps in the anti-discrimination law.

Another key law for genetic privacy in this context is the 21st Century Cures Act, which gives research subjects certain safeguards over their genetic

---

Health Emergency, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 15, 2020),) https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf;; *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 17, 2020), https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html;https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html; Office of Civil Rightshttps://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf; , *COVID-19 and HIPAA: Disclosures to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities*, U.S. DEPT. HEALTH & HUM. SERVS., https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf; Office of Civil Rights, *Civil Rights, HIPAA, and the Coronavirus Disease 2019 (COVID-19)*, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 28, 2020), https://www.hhs.gov/sites/default/files/ocr-bulletin-3-28-20.pdf; Office of Civil Rights, *FAQs on Telehealth and HIPAA During the COVID-19 Nationwide Public Health Emergency*, U.S. DEPT. HEALTH & HUM. SERVS., https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf.

[88] Mason Marks & Tiffany Li, *DNA Donors Must Demand Stronger Protection for Genetic Privacy*, STAT (May 30, 2018), https://www.statnews.com/2018/05/30/dna-donors-genetic-privacy-nih; Megan Molteni, *The US Urgently Needs New Genetic Privacy Laws*, WIRED (May 1, 2019), https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws. https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws/; https://www.statnews.com/2018/05/30/dna-donors-genetic-privacy-nih/

[89] Mason Marks & Tiffany Li, *DNA Donors Must Demand Stronger Protection for Genetic Privacy*, STAT (May 30, 2018), https://www.statnews.com/2018/05/30/dna-donors-genetic-privacy-nih; Megan Molteni, *The US Urgently Needs New Genetic Privacy Laws*, WIRED (May 1, 2019), https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws.,

[90] Ifeoma Ajunwa, *Genetic Testing Meets Big Data: Torts and Contract Law Issues*, 75 OHIO ST. L.J. 1225 (2014).

[91] Ifeoma Ajunwa, *Genetic Data and Civil Rights*, 51 HARV. C.R.-C.Rights- Civil L. L. REV. 75 (2016).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

information in the context of federally funded research.[92] The 21st Century Cures Act includes, for example, that certain researchers "shall not disclose or provide any other person not connected with the research the name of [patient or test subject] or any information, document, or biospecimen that contains identifiable, sensitive information about such an individual and that was created or compiled for purposes of research."[93] However, disclosure of the protected types of information is still allowed under certain conditions, including "for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research"[94] as well as if the disclosure if "made with the consent of the individuals to whom the information, document, or biospecimen pertains."[95] It is also important to note that the privacy protections for research subjects, patients, and data donors under the 21st Century Cures Act includes a limitation that limits the use of "identifiable, sensitive information" in legal process, including preventing such information from being admissible as evidence.[96]

Thus, if genetic information is collected as part of the coronavirus testing data lifecycle, there are a few specific contexts where genetic privacy legal protections would apply. However, with GINA and the 21st Century Cures Act, as with HIPAA, consent is a qualifying exception that can eliminate privacy protections in many cases. It is quite possible that a research subject (e.g., person getting a COVID-19 test as part of a larger medical-research study) could sign away their rights without fully understanding the scope of their consent. Furthermore, these laws protect against discrimination and against specific types of data transfer. They do not protect broader privacy rights.

Outside the U.S. federal context, other jurisdictions also often create special regulations for health data, biometric data, or genetic data. For example, the E.U.'s General Data Protection Regulation regards health data as a special category, thus necessitating special protections for collection and processing.[97] A number of U.S. states also have particular laws that govern biometric and health information, including the Illinois Biometric Information Protection Act (BIPA).[98] BIPA is currently one of the strongest biometric privacy laws in the United States. Under BIPA, businesses that collect biometric information must receive written consent from individuals before data collection, and they must provide notice on policies for data usage and retention. Critically, BIPA allows

---

[92] 42 U.S.C. §USC 201 (2018).

[93] 42 U.S.C. § 241(d)(1)USC 201(B) (2018).

[94] 42 U.S.C. §USC 241(d)(1)(C)(iv) (2018).

[95] 42 U.S.C. § 241(d)(1)USC 201 (C)(iii) (2018).

[96] 42 U.S.C. § 241(d)(1)USC 201 (E) (2018).

[97] Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1, Recital 35.

[98] 740 ILL. COMP. STAT. ILCS14 (2019).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

for a private right of action. Other states are also considering similar legislation.

b. Regulating by Actor and Setting

Some data processors and controllers in the testing-data lifecycle would be considered covered entities under HIPAA, GINA, or other laws and regulations. Many public institutions, particularly public-health institutions, would find themselves regulated by one or more of these laws and regulations. However, as noted, many health-privacy laws have gaps—the most glaring of which is the lack of accountability for private actors, especially actors that are not traditionally healthcare providers.

For private data controllers and data processors, the FTC has broad authority over privacy practices.[99] The common way the FTC has held companies to account over privacy violations has been to note where companies have failed their publicly stated obligations and promises to consumers, thus falling under the FTC's purview to enforce rules on unfair or deceptive practices.[100] Data collectors like 23andMe and private research or health companies could be subject to FTC jurisdiction and thus enforcement in this way. The FTC also has broad enforcement authority over companies that engage in unfair, misleading, or fraudulent activity, which would include any testing actors that misrepresent their testing capabilities or other abilities, in addition to and including privacy or security practices. State attorneys general also have authority to bring actions against companies for privacy violations as well as unfair practices or misleading or fraudulent activity.

No system is perfectly secure, and every actor in the data lifecycle has the potential for suffering a data breach. If this were to happen, state data breach laws would likely apply. In case of data breach, companies could be found to have violated their obligations under HIPAA's Security Rule and Breach Notification Rule, as well as their obligations to act in ways that are not misleading or unrepresentative of their stated practices (thus triggering FTC enforcement). For organizations not covered under HIPAA, the FTC Health Breach Notification Rule[101] requires compliance with notification procedures in case of data breach related to health information. Additionally, other parties involved in the data lifecycle may have a claim against the breached party, on the basis that the breached party failed in its contractual obligations to other parties.

---

[99] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).);

[100] *See, e.g.,* https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were

[101] 16 C.F.R. 318 (2019).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Many of the harms from COVID-19 testing relate to downstream data usage. Here, the law provides far less protection.[102] On a fundamental level, it is difficult for individuals to know exactly where their data goes, past the initial point of collection, or to grasp the full extent of potential data harms—making it next to impossible for individuals to knowingly consent[103] to all the downstream privacy harms that could occur. Data may be shared, sold, or rented with third parties, that could include other actors within the testing ecosystem as well as unrelated parties, like other research centers for related and unrelated projects, as well as commercial actors, like companies seeking to profit from tailored marketing and behavioral advertising,[104] and government actors, like law-enforcement agencies seeking to use genetic information to identify suspects.[105]

Law enforcement can access data, even health and genetic data, stored in private or public collections, through various means, including simply buying data outright. Data collectors or data holders may also sell or freely share data with law enforcement, which could lead to greater surveillance and related harms, particularly important for marginalized communities. Genetic information is particularly interesting to mention, as the genetic information of any one person could potentially be used to identify many people in their genetic family line. In numerous cases, law enforcement have been able to identify potential suspects by matching DNA samples with DNA data of distant relatives.[106] There are few laws, or even proposed laws, that would protect against these downstream privacy harms.

Few laws even contemplate data brokers, aggregators who buy data from multiple sources, package that data together, and then resell to other parties. The privacy harms of data collection are amplified by the process of aggregation (through what Daniel Solove has called "the multiplier problem"[107]), as data

---

[102] For example, while HIPAA arguably should apply to business associates and business associate subcontractors, in practice, the law is rarely enforced against any actors that are not qualified entities.

[103] Charlotte Tschider, *The Consent Myth: Improving Choice for Patients of the Future*, 96 WASH. U. L. REV. 1505 (2018).

[104] Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273 (2012).

[105] Megan Molteni, *The Key to Cracking Cold Cases Might Be Genealogy Sites*, WIRED (June 1, 2018), https://www.wired.com/story/police-will-crack-a-lot-more-cold-cases-with-dna.

[106] Megan Molteni, *The Key to Cracking Cold Cases Might Be Genealogy Sites*, WIRED (June 1, 2018), https://www.wired.com/story/police-will-crack-a-lot-more-cold-cases-with-dna.

[107] Daniel J. Solove, *Why the Law Often Doesn't Recognize Privacy and Data Security Harms*, TEACHPRIVACY (July 9, 2014), https://teachprivacy.com/law-often-doesnt-recognize-privacy-data-security-harms.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

becomes more identifiable with more data from other sources.[108] For example, a company like 23andMe could collect symptom information from its consumers, match that with the genetic information from its database, and sell that to a third party data broker. That data broker could purchase the data and resell it to insurers who could then identify which people, or which groups of people, would be more likely to contract COVID-19, then increasing the rates for insurance for those people. These downstream data harms are especially problematic given the likelihood of future connected health technologies, both public and private, including what Andrea Matwyshyn has termed the "Internet of Bodies."[109] There are no federal laws, and only a few state laws and proposals, that deal with data brokers specifically. U.S. laws do not protect against these downstream, distributed harms. Furthermore, even where law could regulate against these harms, there has often been a lack of strong enforcement actions by regulators.

B. Immunity Passports and Verification Mechanisms

A number of people have proposed using immunity passports or certificates that would indicate someone has developed antibody resistance to COVID-19.[110] In April 2020, Germany began conducting Europe's first nationwide COVID-19 antibody testing program.[111] Researchers at the Hemholtz Centre for Infection Research in Braunschweig proposed a project which would include

---

[108] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013)..,

[109] Andrea M. Matwyshyn, *The Internet of Bodies*, 61 WILLIAM & MARY LAW REVIEW 1 (2019).

[110] *See, e.g.*, Aaron Edlin & Bryce Nesbitt, *The 'Certified Recovered' from Covid-19 Could Lead the Economic Recovery*, STAT (Apr. 6. 2020), https://www.statnews.com/2020/04/06/the-certified-recovered-from-covid-19-could-lead-the-economic-recovery; Opinion, Ezekiel J. Emanuel, *We Can Safely Restart the Economy in June. Here's How.*, N.Y. TIMES (Mar. 28, 2020), https://www.nytimes.com/2020/03/28/opinion/coronavirus-economy.html; Jason Horowitz, *In Italy, Going Back to Work May Depend on Having the Right Antibodie*s, N.Y. TIMES (Apr. 4, 2020),https://www.washingtonpost.com/health/2020/03/31/coronavirus-serology-blood-tests/; https://www.nytimes.com/2020/04/04/world/europe/italy-coronavirus-antibodies.html; Veronika Hackenbroch, *Große Antikörperstudie Soll Immunität Der Deutschen Gegen Covid-19 Feststellen*, DER SPIEGEL (Mar. 27, 2020), https://www.spiegel.de/wissenschaft/medizin/coronavirus-grosse-antikoerper-studie-soll-immunitaet-der-deutschen-feststellen-a-c8c64a33-5c0f-4630-bd73-48c17c1bad23; Carolyn Y. Johnson, *Testing Coronavirus Survivors' Blood Could Help Reopen U.S.*, WASH. POST (Mar. 31, 2020, 12:35 PM EDT),https://www.nytimes.com/2020/04/04/world/europe/italy-coronavirus-antibodies.html; https://www.washingtonpost.com/health/2020/03/31/coronavirus-serology-blood-tests.https://www.statnews.com/2020/04/06/the-certified-recovered-from-covid-19-could-lead-the-economic-recovery/;

[111] Rob Schmitz, *Germany Is Conducting Nationwide COVID-19 Antibody Testing*, NPR (Apr. 21, 2020), https://www.npr.org/sections/coronavirus-live-updates/2020/04/21/839594202/germany-is-conducting-nationwide-covid-19-antibody-testing.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

mass testing for antibodies as well as immunity certificates ("similar to a vaccination certificate"[112]) that would allow people certain exceptions from COVID-19 restrictions, e.g., limitations on travel or non-essential work.[113] Scientists in Italy have also proposed similar programs, as has New York Governor Andrew Cuomo.[114]

Immunity passports or certificates come with many issues, including privacy. Immunity verification requires testing to determine the presence of antibodies that could imply immunity (temporary or permanent). As discussed above, testing in general generates a host of privacy issues, regardless of which party is collecting, processing, sharing, or controlling the data. Requiring or encouraging immunity verification for employment, housing, education, or even for entering a movie theater or shopping center could lead to an increase in testing, and thus a compounding of the privacy harms related to testing. Electronic transfer of immunity-related data also raises privacy risks, which may necessitate new guidelines around HIPAA and other laws that govern health information (potentially including Americans with Disabilities Act (ADA) limitations for employee data as well). Regulations have already been relaxed during pandemic.[115]

---

[112] Lydia Smith, *Germany to Introduce Coronavirus 'Immunity Certificates' for Recovered Public*, NEWSWEEK (Mar. 30, 2020), https://www.newsweek.com/germany-antibodies-tests-general-public-immunity-certificates-1494934 (quoting in translation https://www.spiegel.de/wissenschaft/medizin/coronavirus-grosse-antikoerper-studie-soll-immunitaet-der-deutschen-feststellen-a-c8c64a33-5c0f-4630-bd73-48c17c1bad23).

[113] Lydia Smith, *Germany to Introduce Coronavirus 'Immunity Certificates' for Recovered Public*, NEWSWEEK (Mar. 30, 2020), https://www.newsweek.com/germany-antibodies-tests-general-public-immunity-certificates-1494934.

[114] Jason Horowitz, *In Italy, Going Back to Work May Depend on Having the Right Antibodie*s, N.Y. TIMES (Apr. 4, 2020), https://www.nytimes.com/2020/04/04/world/europe/italy-coronavirus-antibodies.html.

[115] *See, e.g.*, *COVID-19 & HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public*

Health Emergency, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 15, 2020), https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf; *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 17, 2020), https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html; Office of Civil Rights, *COVID-19 and HIPAA: Disclosures to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities*, U.S. DEPT. HEALTH & HUM. SERVS., https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf; Office of Civil Rights, *Civil Rights, HIPAA, and the Coronavirus Disease 2019 (COVID-19)*, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 28, 2020), https://www.hhs.gov/sites/default/files/ocr-bulletin-3-28-20.pdf; Office of Civil Rights, *FAQs on Telehealth and HIPAA During the COVID-19 Nationwide Public Health Emergency*, U.S. DEPT. HEALTH & HUM. SERVS., https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Encouraging testing for immunity verification can lead to individuals feeling compelled to take tests, regardless of their concerns over privacy or other issues. People may feel compelled to participate in testing, particularly if testing is necessary for immunity verification that can lead to employment. This lack of control over personal health data could be harmful for privacy, or at least to a person's perception of their own control over personal privacy. Normalizing this form of widespread testing and sharing of private health or genetic data with multiple corporate and government interests could also create change in our society's expectations of privacy, with harmful consequences for future privacy norms and laws.

Conditioning employment, housing, education, travel, or other rights and privileges on immunity verification could have dangerous consequences. Immunity passport or verification programs could create a lasting shift in social norms, laying the groundwork for future programs that use genetics or health status as conditions for accessing certain rights and privileges. On the extreme end, this line of argumentation could be used to justify programs that edge close to eugenics,[116] privileging some based on health, physical ability, or innate genetic characteristics. Normalizing immunological discrimination could pave the way for a loosening of discrimination laws and practices generally, particularly related to health discrimination, as well as for certain sectors, like employment.

These problems with immunity passports have historical antecedents. Kathryn Olivarius has written about the complex interplay between health and capital in the "immunocapital" economy of the Yellow Fever epidemic of the early 1900s.[117] Connecting the past immunity economy to the proposed immunity passports of the COVID-19 era, Olivarius writes:

> Immunity on a case-by-case basis *did* permit the economy to expand, but it did so unevenly: to the benefit of those already atop the social ladder, and at the expense of everyone else. When a raging virus collided with the forces of capitalism, immunological discrimination became just one more form of bias in a region already premised on racial, ethnic, gender and financial inequality.[118]

Widespread immunity verification programs could effectively create the

---

[116] *Godwin's Law*, WIKIPEDIA, https://en.wikipedia.org/wiki/Godwin's_law.

[117] Kathryn Olivarius, *Immunity, Capital, and Power in Antebellum New Orleans*, 124 AM. HIST. REV. 425 (2019).

[118] Kathryn Olivarius, The *Dangerous History of Immunoprivilege*, N.Y. TIMES (Apr. 12, 2020), https://www.nytimes.com/2020/04/12/opinion/coronavirus-immunity-passports.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

"immunological discrimination" Olivarius describes, leading to discriminatory effects on marginalized and disadvantaged groups. For example, if some jobs are conditioned on immunity verification, people might be willing to voluntarily infect themselves with COVID-19 in order to gain the immunity, and by proxy, the immunity verification needed for employment. This particular risk to individual health would likely be greater for the unemployed and underemployed, and other people who would find the financial incentive strong enough to overcome the risks to their own health. As Olivarius notes, the use of immunity verification as condition for employment shifts the burden on the working classes to become "acclimated" to the virus, not on those in power to invest in societal infrastructure.[119]

Additionally, immunity testing and verification may not be available equally to all people. For example, people who lack medical insurance (particularly in countries like the United States, without free or low-cost public healthcare) may be unwilling or unable to get the testing needed to receive immunity verification. Thus, if immunity verification were to become a standard, already disadvantaged people would not be able to access the same benefits from immunity verification that others would.

Black people, indigenous people, and people from other marginalized groups may have greater resistance to enrolling in any public health database or government data collection program, without strong assurances that their data will not be used against them and their communities, given historical examples of the law enforcement overreach. For example, some may fear that their genetic material will be accessible by law enforcement, as has been shown through government use of commercial DNA databases,[120] which could result in threatening consequences for groups who already disproportionately suffer from the effects of institutional and structural racism in public health and policing. Undocumented people may fear that their genetic data will be used to link them to other undocumented people, thus leading to harmful immigration consequences for themselves and their loved ones.[121] They, too, would not be able to benefit from immunity verification.

---

[119] Kathryn Olivarius, The *Dangerous History of Immunoprivilege*, N.Y. TIMES (Apr. 12, 2020), https://www.nytimes.com/2020/04/12/opinion/coronavirus-immunity-passports.html.

[120] Mason Marks & Tiffany Li, *DNA Donors Must Demand Stronger Protection for Genetic Privacy*, STAT (May 30, 2018), https://www.statnews.com/2018/05/30/dna-donors-genetic-privacy-nih.

[121] Megan Molteni, *How DNA Testing at the US-Mexico Border Will Actually Work*, WIRED (May 2, 2019), https://www.wired.com/story/how-dna-testing-at-the-us-mexico-border-will-actually-work; *DNA Tests at Border: DHS to Start Testing to Catch People Posing as Families*, CBS DENVER (May 2, 2019),https://www.wired.com/story/how-dna-testing-at-the-us-mexico-border-will-actually-work/; https://denver.cbslocal.com/2019/05/02/dna-tests-border-department-homeland-security.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Using immunity verification as a limiting factor for fundamental rights like employment, education, and travel could raise constitutional issues as well, though it is arguable that the government's compelling interest in protecting public health in the middle of an active pandemic could outweigh many potential concerns at least for limited, short term programs. However, as the legal and regulatory landscape surrounding immunity passports is extremely bare, it would be difficult for anyone to challenge an incorrect immunity verification and defend their rights. This difficulty in contestation would be especially pronounced for those who lack the resources and access to legal support. Furthermore, it is likely that any programs that develop during pandemic response will have lasting effects on laws and norms for the future.

Current U.S. discrimination law likely does not prevent the use of immunity verification programs like immunity passports. The Genetic Information Nondiscrimination Act of 2008 (GINA) protects individuals against discrimination based on genetic information, but this law is limited to two sectors: health insurance and employment. GINA prevents health insurers from denying coverage to individuals based on genetic predisposition and prevents employers from using genetic information for hiring, firing, promotion, and related employment decisions.

While it might seem that GINA would protect genetic privacy in the context of testing and immunity passports, this may not be the case. GINA does not protect employees from employer surveillance of their genetic information, potentially including information related to coronavirus testing or immunity verification. Furthermore, GINA allows employers to request, require, or purchase genetic information of employees in certain circumstances, including to comply with certification requirements of the Family and Medical Leave Act and other leave laws and policies, as well as genetic monitoring programs required by law as well, as well as data from sources that are commercially and publicly available, and data that an employee voluntarily consents to giving. While employers are generally prevented from sharing or exposing genetic information, they are allowed to do so under some circumstances. Additionally, it is unclear if immunity information would fall under the scope of GINA, as the information included in an immunity verification passport could potentially exclude genetic information.

Particularly important is the fact that GINA does not include a cause of action for genetic discrimination based on disparate impact, a failing Ifeoma Ajunwa has noted. Ajunwa argues that such a clause should be added to GINA because:

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

> (1) ease of access to genetic testing and the insecurity of genetic information has increased the likelihood of genetic discrimination in employment;
>
> (2) the addition of a disparate impact clause is in line with the precedent set by prior employment discrimination laws;
>
> (3) the EEOC has declared that proof of deliberate acquisition of genetic discrimination is not necessary to establish a violation of GINA, likewise, proof of intent to discriminate should not be required to demonstrate that there has been genetic discrimination;
>
> (4) and finally, real world instances of genetic testing have shown that facially neutral testing may result in racial disparities.[122]

Adding a disparate-action clause to GINA would protect against most of the genetic discrimination harms raised by the use of genetic information in the modern, Big Data era, outside of the limited contexts GINA currently governs. With the greater scale of testing data, the insecurity of genetic information has likely increased the likelihood of genetic discrimination, particularly enhanced by the concept of conditioning employment on immunity verification. Adding a disparate impact clause would be in line with prior precedent, and past EEOC declarations remain current. Perhaps most importantly, there is historical precedent for the racial disparities and discriminatory impact of genetic testing based on immunity.[123]

If GINA, the law specifically concerning genetic discrimination, might not fully protect genetic privacy rights for individuals in the context of immunity passports, one might wonder if the ADA would serve. The ADA protects against discrimination in many contexts, including employment. However, here again, the ADA is insufficient to protect individuals from the discriminatory harms of enforced immunity-verification programs. The ADA allows employers to screen out individuals by applying qualification standards, which could include the requirement "that an individual shall not pose a direct threat to the health or safety of other individuals in the workplace."[124] Employers are also allowed to conduct "voluntary medical examinations, including voluntary medical histories" and "make inquiries into the ability of an employee to perform job-related functions."[125] In fact, the EEOC in May released guidance

---

[122] Ifeoma Ajunwa, *Genetic Data and Civil Rights*, 51 HARV. C.R.-C.L. L. REV. 75, 79 (2016).

[123] Kathryn Olivarius, *Immunity, Capital, and Power in Antebellum New Orleans*, 124 AM. HIST. REV. 425 (2019); Kathryn Olivarius, The *Dangerous History of Immunoprivilege*, N.Y. TIMES (Apr. 12, 2020), https://academic.oup.com/ahr/article/124/2/425/5426380?guestAccessKey=147da8dd-81f0-4820-84eb-a766c4c8f74f; https://www.nytimes.com/2020/04/12/opinion/coronavirus-immunity-passports.html.

[124] 42 U.S.C. § 12113(b) (2018).

[125] 42 U.S.C. § 12112(d)(4)(B) (2018).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

on interpreting ADA protections in light of the COVID-19 pandemic, and suggested that employers may institute testing of employees for exposure to the virus.[126]

To address the harms of genetic discrimination raised by COVID-19 testing and immunity-verification proposals, we must strengthen protections in GINA and the ADA. This can come through new genetic-privacy laws,[127] through genetic-privacy provisions in a future national privacy law, or perhaps in an algorithmic-discrimination or algorithmic-accountability law, as the privacy harms of new technologies are heavily amplified by the impacts of Big Data, machine learning, and artificial-intelligence systems today.

C. Contact Tracing

In addition to testing for coronavirus exposure, states have also turned to contact tracing programs as key parts of pandemic response. Contact tracing in this context refers to the practice of tracing the contacts of a person identified as having been exposed to COVID-19, in an effort to halt the further onward spread of the virus.[128]

Contact tracing attempts to quickly track and stop the spread of COVID-19 by starting with each person who tests positive for the virus. When a person is infected with a virus like COVID-19, the infected person is contagious for a period of time. During this time, the infected person is able to infect others with the virus. People who come in close physical contact with that person ("contacts") thus have a higher risk of infection. Contact tracing attempts to identify these people quickly, so that the contacts of the infected person can take steps to also get tested and to practice social isolating, to prevent potentially infected contacts from spreading the virus further.

1. Contact Tracing Principles

Contact tracing starts with confirming a person has or had a COVID-19

---

[126] *What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws*, U.S. EQUAL EMP. OPPORTUNITY COMMISSION, https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

[127] *But see* Sonia M. Suter, *The Allure and Peril of Genetic Exceptionalism: Do We Need Special Genetics Legislation?*, 79?. WASH. U. L.Q. 669 (2001).Review

[128] Selena Simmons-Duffin, *How Contact Tracing Works and How It Can Help Reopen the Country*, NPR (Apr. 14, 2020), https://www.npr.org/sections/health-shots/2020/04/14/833726999/how-contact-tracing-can-help-fight-coronavirus; *Contact Tracing*, WORLD HEALTH ORG. (May 9, 2017), https://www.who.int/news-room/q-a-detail/contact-tracing.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

viral infection. Contact tracing is then implemented to study and stop the further spread of the virus by alerting the infected person to isolate and by alerting all people who may have been in contact with the infected person to also monitor their own symptoms and isolate if needed.

The World Health Organization breaks down contact tracing into three basic steps: (1) contact identification; (2) contact listing; and (3) contact follow-up.[129] In contact identification, steps are taken to identify all the individuals that may have been in contact with a person who had the COVID-19 virus during the period of potential viral transmission. In contact listing, contacts are informed of their contact status as well as steps they should take to protect their own health and the health of others. In contact follow-up, contact tracing program administrators follow up with contacts to monitor for symptoms and test for signs of infection.

Different types of contact tracing programs have emerged in response to the novel coronavirus pandemic: human contact tracing and digital contact tracing. Digital contact tracing has come in two primary conceptions: Bluetooth-based, "decentralized" contact tracing, and centralized contact tracing, often through cell-phone location data or also through Bluetooth-based data. Each of these forms of contact tracing programs has its own portfolio of privacy concerns, and different states have implemented one or more of them. Thus, it is necessary to discuss each form of contact tracing program in order to attempt to grasp a holistic overview of the privacy issues raised by contact tracing in the midst of the COVID-19 pandemic.

Contact tracing is not a new concept but rather an accepted and tested process used in a variety of epidemiology and public health contexts. However, the technologies used for digital contact tracing are new and relatively untested at scale, and these new technologies raise interesting societal issues. The clash between human and digital contact tracing also brings to light debates regarding automation and the ability to use machines to replicate or replace human work. Additionally, the privacy and security problems with digital contact tracing proposals reflect the changing nature of our society's relationship with digital privacy, and the ways in which Big Data and the increasingly imbalanced nature of the data economy have shaped consumer expectations of privacy.

2. Human Contact Tracing

Governments around the world have implemented mass contact-tracing programs. For example, the state of Massachusetts created a statewide contact-

[129] *Contact Tracing*, WORLD HEALTH ORG. (May 9, 2017), https://www.who.int/news-room/q-a-detail/contact-tracing.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

tracing program, hiring 1,000 new contact tracers as part of human contact-tracing programs.[130] The city of San Francisco launched a program training 150 volunteers to add to the existing contact-tracing programs from their city public-health department.[131]

Human contact tracing, or manual contact tracing, refers to contract tracing done through manual identification of contacts through non-automated means, as well as contact listing and contact follow-up done through manual, non-automated means. Traditionally, contact tracing has meant contact tracing as done manually by humans. However, with this global pandemic in an age of increasingly digitized services, contact tracing through automated technologies has emerged as a contender, for better or worse.

a. Human Contact Tracing Data Lifecycle

Human contact tracing describes a process that has been used in epidemiological and public health contexts prior to but also including the COVID-19 pandemic. The process is as follows[132]:

First, a confirmed infected person speaks to a contact tracer, a person fulfilling a contact tracing role. In this conversation, the contact tracer asks questions of the infected person, with an eye toward identifying contacts. These conversations often take place in a one-on-one setting over the phone. For example, a contact tracer from a state health department could call a person who tested positive of COVID-19 and ask for a list of everyone the infected person had come into contact with in the last 2 weeks.

Contact tracers can be healthcare professionals, public health workers, or dedicated contact tracing staff. In Massachusetts, which launched a robust human contact tracing program, this identification stage is done through one-on-one calls between the infected person and a contact tracer (hired by the state program, in partnership with a medical nonprofit, Partners in Health).[133] Contact

---

[130] Ellen Barry, *An Army of Virus Tracers Takes Shape in Massachusetts*, N.Y. TIMES (Apr. 16, 2020), https://www.nytimes.com/2020/04/16/us/coronavirus-massachusetts-contact-tracing.html.

[131] Kristen Sze, *EXCLUSIVE: San Francisco Launches Initiative to Trace Every Single COVID-19 Case and Contact*, ABC7 NEWS (Apr. 9, 2020), https://abc7news.com/san-francisco-contact-tracing-coronavirus-tracnig-bay-area-lockdown-shelter-in-place/6090943.

[132] Selena Simmons-Duffin, *How Contact Tracing Works and How It Can Help Reopen the Country*, NPR (Apr. 14, 2020), https://www.npr.org/sections/health-shots/2020/04/14/833726999/how-contact-tracing-can-help-fight-coronavirus.

[133] Ellen Barry, *An Army of Virus Tracers Takes Shape in Massachusetts*, N.Y. TIMES (Apr. 16, 2020), https://www.nytimes.com/2020/04/16/us/coronavirus-massachusetts-contact-tracing.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

tracers receive information about infected persons through state databases that store results of coronavirus tests. The contact tracer then calls the infected person by phone and creates a list of all people the person had been in contact with in the 48 hours before the person's symptoms began.

Second, contact tracers will call or otherwise notify all contacts that they were exposed to someone who tested positive of COVID-19, informing these contacts of their risks as well as how to protect themselves and others from the virus and its effects. Contact tracers may suggest that contacts perform such actions as monitoring their own symptoms, self-quarantining, or trying to get their own tests for viral infection. In the Massachusetts contact tracing program, contact tracers attempt to call each contact, calling three times in succession "to signal the call's importance."[134] If the contact picks up the phone, the contact tracer then informs them that they may have been expose to the virus, walks them through common symptoms and quarantine recommendations, and explains where they can get further help if needed. These conversations can take thirty to forty minutes.[135]

In an ongoing final stage of the process, contact tracers follow up with contacts to monitor symptoms and spread of the virus. This can be done informally or through rigorously monitored programs. In South Korea,[136] for example, contact tracers follow up with contacts on a routine basis and request or mandate that contacts track and submit their symptoms to a government database.

Human contact tracing has its benefits and drawbacks, when compared to digital contact tracing programs. Finding out that you may have been exposed to the virus can be a frightening or worrying experience, and it can be helpful to have a human there to guide that first conveying of information. Public-health officials, taking lessons from contact tracing sexually transmitted infections such as HIV, have learned "to talk to people in a way that's not stigmatizing and will encourage people to get on board with the request to self-isolate or share their contacts," according to Jeff Engel, senior advisor for COVID-19 to the Council

---

[134] Ellen Barry, *An Army of Virus Tracers Takes Shape in Massachusetts*, N.Y. TIMES (Apr. 16, 2020), https://www.nytimes.com/2020/04/16/us/coronavirus-massachusetts-contact-tracing.html.

[135] Ellen Barry, *An Army of Virus Tracers Takes Shape in Massachusetts*, N.Y. TIMES (Apr. 16, 2020), https://www.nytimes.com/2020/04/16/us/coronavirus-massachusetts-contact-tracing.html.

[136] Max S. Kim, *South Korea is Watching Quarantined Citizens with a Smartphone App*, MIT TECH. REV. (Mar. 6, 2020), https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

of State and Territorial Epidemiologists.[137] It is likely that an automated process cannot duplicate the social and emotional benefits of human contact tracing, perhaps similar to the same issues we see with the use of care robots in times of crisis.

It is difficult to calculate the social benefit of having human contact in the contact tracing process. However, it is possible to calculate the financial costs of contact tracing programs, which some governments may find too expensive.[138] On the other hand, hiring unemployed individuals to serve as contact tracers could create an economic stimulus in a time when unemployment is high. Perhaps the greatest flaw of the human contact-tracing programs isn't the cost but the difficulty of scaling a personal, one-to-one approach to a global pandemic.

b. Human Contact Tracing's Privacy Impact

For a holistic analysis of the privacy issues related to human contact tracing, we can start once again with the types of data that are collected and processed, as well as the different actors involved with contact tracing.

Contact tracers receive information about the infected person to facilitate the contact identification stage (e.g., phone interviews). This information can include name, phone number, address, as well as health information (at the very least, a positive COVID-19 test result). During the identification conversations, infected persons may share the names and contact information of potential contacts, as well as other information, including information about the infected person's activities and locations in the days prior to the start of their symptoms. As these are phone calls between two potentially unpredictable human beings, any number of other types of information could be shared in the identification stage. Similarly, in the contact listing stage, which consists of conversations with contacts, many types of data may be shared—including identifying information as well as others.

Some of the information collected during human contact tracing can include health information, as defined in HIPAA and state laws. Contact tracers may be acting on behalf of entities that would be governed under HIPAA, including healthcare providers, which could mean that transmission of health information

---

137 Selena Simmons-Duffin, *How Contact Tracing Works and How It Can Help Reopen the Country*, NPR (Apr. 14, 2020), https://www.npr.org/sections/health-shots/2020/04/14/833726999/how-contact-tracing-can-help-fight-coronavirus.

138 Ellen Barry, *An Army of Virus Tracers Takes Shape in Massachusetts*, N.Y. TIMES (Apr. 16, 2020), https://www.nytimes.com/2020/04/16/us/coronavirus-massachusetts-contact-tracing.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

would have to comply with HIPAA and similar regulations. Contact tracers may also be acting through state and municipal public-health departments, which would not necessarily be covered entities that have to comply with HIPAA restrictions on health information. However, most of the entities conducting COVID-19 tests would likely qualify as HIPAA covered entities; thus, organizations receiving health information would likely have to at least comply with the requirements for business associates under HIPAA. Laws like GINA and the 21st Century Cures Act protect the confidentiality of patient health information used for federally-funded research.

There are some risks to privacy and security that come with human contact-tracing programs, particularly during a pandemic in which many would work from home. The more people have access to any data (including health information), the more risk there is that data may be exposed, even inadvertently. As it is likely many contact tracers may work remotely, it may be difficult to monitor whether contact tracers are practicing strong cybersecurity hygiene in protecting information. For example, it is difficult to know if any contact tracers are separately recording or writing down information from conversations, or if there are other people in the room while the contact tracer is working. It is possible that digital contact-tracing programs could have less of this form of distributed risk, as well as less room for human error contributing to privacy and security risks. There are a number of data breach disclosure laws across states that may come into play if information were to be exposed.

3. Digital Contact Tracing

In the COVID-19 pandemic, digital contact tracing has emerged as a public-health response tool, for perhaps the first time on such a large national and global scale.[139] In contrast to human contact tracing, digital contact tracing relies on digital, often automated, "contact tracing apps" that aid in identifying potential contacts of infected individuals. Digital contact tracing can also include digital, sometimes app-based, means of informing contacts of their potential exposure and the associated risks and recommendations. The follow-up capabilities of digital contact tracing programs are various and can include simple email reminders to required enrollment in apps that track symptoms.

Two primary forms of digital contact tracing have become popular:[140] first,

---

[139] Patrick Howell O'Neill, Tate Ryan-Mosley & Bobbie Johnson*, A Flood of Coronavirus Apps Are Tracking Us. Now It's Time*i *to Keep Track of Them.*. MIT TECH. REV. (May 7, 2020), Review.https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker.

[140] Cristina Criddle & Leo Kelion, *Coronavirus Contact-Tracing*contact-tracing*: World Split Between Two Types of App*, BBC (May 7, 2020), https://www.bbc.com/news/technology-52355028.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

a centralized approach, often utilizing cell-phone location data; second, a decentralized approach, often using a short-range Bluetooth standard. Both types of digital contact-tracing programs have their benefits and drawbacks, not the least of which relate to privacy impacts of individuals and groups.

a. Decentralized Digital Contact Tracing

While each proposed digital contact-tracing application is different, generally, decentralized contact-tracing apps use short-range Bluetooth technology to determine proximity between individuals at certain points in time. The concept involves individuals (ideally a high percentage[141] of the populace) downloading the app. Some of these apps would run on background, and some would need to be active on a person's mobile device to be useful. If a person tests positive for COVID-19, that person would update their status with the app (or, in some cases, another entity could update the app). The decentralized digital contact-tracing apps would then utilize "a record of anonymous key codes exchanged between phones" to determine which other individuals (who had the app installed or active) had been in proximity with the infected person during the contagious period.[142]

Decentralized contact-tracing apps have been called "privacy-preserving."[143] These privacy-preserving proposals include the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) project,[144] the East Coast[145] PACT,[146] the

---

[141] *Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease Us Out of Lockdown*, OXFORD (Apr. 16, 2020), https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

[142] Kylie Foy, *Bluetooth Signals From Your Smartphone Could Automate Covid-19 Contact Tracing While Preserving Privacy*, MIT NEWS (Apr. 8, 2020), https://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409.

[143] For example, the ACLU released a white paper on digital contact tracing that specifically noted DP-3T, East Coast PACT, and TCN as privacy-preserving proposals. Daniel Kahn Gillmor, *Principles for Technology-Assisted Contact-Tracing*, AM. C.L. UNION (Apr. 16, 2020), https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing.

[144] *Decentralized Privacy-Preserving Proximity Tracing*, GITHUB, https://github.com/DP-3T.

[145] Informal differentiation suggested by the team behind the "East Coast PACT," upon noting the accidental similarity in acronym. *See* Ronald L. Rivest et al., *The PACT Protocol Specification*, PACT (Apr. 8, 2020), https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf.

[146] PACT: PRIVATE AUTOMATED CONTACT TRACING, https://pact.mit.edu; Ronald L. Rivest et al., *PACT: Private Automated Contact Tracing* (Apr. 7, 2020), https://pact.mit.edu/wp-content/uploads/2020/04/MIT-PACT-ONEPAGER-2020-04-07-B.pdf; Ronald L. Rivest et al., *The PACT Protocol Specification*, PACT (Apr. 8, 2020), https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

West Coast PACT,[147] and TCN.[148] European states and researchers have supported the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT).[149] These decentralized digital contact-tracing apps all have similarities in their protocol design.[150] Some researchers involved with these apps have suggested solutions for increasing interoperability, allowing solutions to develop in parallel and potentially exchange information (e.g., users of multiple apps would be pinged if they were found to have been in proximity with an infected person), aiding widespread adoption and use.[151]

Perhaps the leading commercial proposal is an approach developed by Apple and Google in partnership.[152] Through the joint effort, Apple and Google launched a "comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing."[153] An API is a computer-programing interface that defines interactions between software components or applications, allowing applications to call and request data. The Apple and Google proposal performs a different function than the other decentralized digital contact-tracing proposals, in that it provides an API that can be used to allow communication between other applications, as opposed to releasing an application that can stand on its own. Google and Apple specify this as an "Exposure Notification system," rather than a contact-tracing application,[154] perhaps for that reason.

Some nations and states have deployed contact tracing apps. However, these apps have not reached a high percentage of the population in most regions where the apps have launched. For example, as of July 2020, only 14.4% of the

---

[147] Justin Chan et al., PACT: Privacy-Sensitive Protocols and Mechanisms for Mobile Contact Tracing (May 7, 2020) (unpublished manuscript), https://arxiv.org/pdf/2004.03544.pdf.

[148] TCN COALITION, https://tcn-coalition.org.

[149] PAN-EUROPEAN PRIVACY-PRESERVING PROXIMITY TRACING, https://www.pepp-pt.org.

[150] Ronald L. Rivest et al., *The PACT Protocol Specification*, PACT (Apr. 8, 2020), https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf.

[151] Ellie Daw et al., *Contact Tracing Interoperability Recommendations*, TCN COALITION (May 1, 2020), https://tcncoalition.files.wordpress.com/2020/05/tcncoalition_interoperability_recommendations_whitepaper.pdf.

[152] *Apple and Google Partner on COVID-19 Contact Tracing Technology*, GOOGLE (Apr. 10, 2020), https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology.

[153] *Apple and Google Partner on COVID-19 Contact Tracing Technology*, GOOGLE (Apr. 10, 2020), https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology.

[154] Privacy-Preserving Contact Tracing, APPLE, https://www.apple.com/covid19/contacttracing.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

population in Germany downloaded the state-developed "Corona-Warn-App," and only 4% of the population in France have downloaded the similar "StopCovid" app.[155] It appears likely that digital contact tracing will not be a large factor in solving the coronavirus pandemic. However, with the launch of these apps, it is likely that the next major epidemic will involve digital contact tracing. Thus, it is important to understand how these apps function in this crisis, to better prepare for the next one.

b. Centralized Digital Contact Tracing

Centralized digital contact-tracing apps diverge from decentralized apps in relying on a central database or central authority for the contact-tracing data and process.[156] For example, Singapore's Trace Together app collects all data from individual devices in a national-government database[157].

Centralized contact-tracing app proposals have involved a variety of data sources, primarily Bluetooth data and cell-phone location data. For example, a Bluetooth-based decentralized app would infer proximity through anonymous key exchange device-to-device; but a Bluetooth-based centralized app could infer proximity through keys stored on a central database, with data collected from each device and results pushed back to devices.

The chief privacy concern with centralized contact tracing is that these programs would enable governments to collect and use data as part of large-scale surveillance, with few limits on what governments could do with the data.[158] With centralized digital contact tracing, a central authority has control over all data that is collected, used, shared, and stored. There are few protections against misuse of data collected by these apps. Thus, the privacy of users of centralized contact-tracing apps depends on the trustworthiness of the central authority.

However, as Helen Nissenbaum noted on Twitter, "there's no loss of privacy as long as data is appropriately channeled. Trade off language sets up false dilemmas; we can enjoy gains without privacy casualties."[159] Using

---

[155] Gabriel Geiger, *Europeans Aren't Really Using COVID-19 Contact Tracing Apps*, VICE (July 21, 2020), https://www.vice.com/en_uk/article/akzne5/europeans-arent-really-using-covid-19-contact-tracing-apps.

[156] Baobao Zhang et al., *Americans' Perceptions of Privacy and Surveillance in the COVID-19 Pandemic*, OSF PREPRINTS (May 13, 2020), osf.io/9wz3y.

[157] Baobao Zhang et al., *Americans' Perceptions of Privacy and Surveillance in the COVID-19 Pandemic*, OSF PREPRINTS (May 13, 2020), osf.io/9wz3y.

[158] Susan Landau, Christy E. Lopez & Laura Moy, *The Importance of Equity in Contact Tracing*, LAWFARE (May 1, 2020), https://www.lawfareblog.com/importance-equity-contact-tracing.

[159] Helen Nissenbaum (@HNissenbaum), TWITTER (May 13, 2020, 3:13 PM),

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Nissenbaum's influential contextual integrity framework,[160] we can certainly envision a scenario in which privacy rights are protected for the specific contexts raised by the contact-tracing process. In fact, some have argued that centralized contact-tracing apps may be more secure or privacy-protective, in that one central source stores all private information, making it potentially easier to govern the flows of data.

c. Digital Contact Tracing's Privacy Impact

One issue with digital contact tracing apps, whether decentralized or centralized, is that they require a high percentage of the population to download and use the apps in order for the apps to actually be effective in tracing contacts and stopping or slowing the spread of disease.[161] However, early research surveying public perception on various digital contact-tracing apps has revealed mixed results,[162] suggesting that it may be difficult to convince some populations (e.g., certain nations or regions) to adopt the apps at a high enough rate to be efficacious. Indeed, as of July 2020, few if any nations that have rolled out voluntary apps have seen app adoption at rates necessary for effective contact

---

https://twitter.com/HNissenbaum/status/1260649364407545856.

[160] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).

[161] *Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease Us Out of Lockdown*, U. OXFORD (Apr. 16, 2020), https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

[162] *See, e.g.*, Monica Anderson & Brooke Auxier, *Most Americans Don't Think Cellphone Tracking Will Help Limit COVID-19, Are Divided on Whether It's Acceptable*, PEW RES. (Apr. 16, 2020), https://www.pewresearch.org/fact-tank/2020/04/16/most-americans-dont-think-cellphone-tracking-will-help-limit-covid-19-are-divided-on-whether-its-acceptable; Eszter Hargittai et al., *Covid-19 Study on Digital Media and the Coronavirus Pandemic*, WEB USE PROJECT, http://webuse.org/covid; Luke Milsom et al., *Survey of Acceptability of App-Based Contact Tracing in the UK, US, France, Germany and Italy*, OSF (May 12, 2020), osf.io/7vgq9; Baobao Zhang et al., *Americans' Perceptions of Privacy and Surveillance in the COVID-19 Pandemic*, OSF PREPRINTS (May 13, 2020), See, e.g., osf.io/9wz3y; Lucy Simko et al., COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences (May 8, 2020) (unpublished manuscript), https://seclab.cs.washington.edu/wp-content/uploads/2020/05/contact-tracing-user-privacy.pdfhttps://www.pewresearch.org/fact-tank/2020/04/16/most-americans-dont-think-cellphone-tracking-will-help-limit-covid-19-are-divided-on-whether-its-acceptable/;acceptabilityapp-based contact tracing. For a publicly accessible, updated list of studies on perceptions of privacy and contact-tracing apps, see Baobao Zhang, *COVID-19 Contact Tracing Apps Public Opinion Studies*, NOTION,: https://www.notion.so/34e11bad13e34c558f5aa4a4975f6df0?v=c36d57c8ae5640a49a00b91d79a4cf9c.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

tracing.[163] Some nations, like India,[164] have gotten around this by mandating citizens download and use the app.

Several scholars and advocates have expressed concerns about the privacy and civil-liberties harms contact-tracing apps might cause. Woodrow Hartzog noted that, although the Google and Apple proposal might be well-meaning, it would be difficult for the companies to police the use of app operators to ensure compliance.[165] (This is not far-fetched. One need only look at the non-compliance of app developers on the Google Play store or Apple app store, which has been a constant issue for many app platforms.[166]) Hartzog argues it would be simple for governments to abuse even the most privacy-preserving contact-tracing apps and, crucially, "this technology, once deployed, will not be 'rolled back.'"[167]

Susan Landau et al. have also argued that contact-tracing apps may also create a false sense of security, leading some to recklessly put themselves at greater risk of exposure while relying on a potentially ineffective app.[168] Contact-tracing apps also raise equity concerns, as highlighted by Laundau et al., generating more false positives, with worse consequences.[169] Additionally, if data collected through these apps is eventually used for other purposes, including law enforcement, this could have worse impact on some populations.[170] Simko et al. have noted a number of privacy harms, including the potential for malicious actors to create intentional false positives, with negative consequences for people or businesses.[171]

---

[163] Gabriel Geiger, *Europeans Aren't Really Using COVID-19 Contact Tracing Apps*, VICE (July 21, 2020), https://www.vice.com/en_uk/article/akzne5/europeans-arent-really-using-covid-19-contact-tracing-apps.

[164] Patrick Howell O'Neill, *India Is Forcing People to Use Its Covid App, Unlike Any Other Democracy*, MIT TECH. REV. (May 7, 2020), https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory.

[165] Opinion, Woodrow Hartzog, *Op-Ed: Coronavirus Tracing Apps Are Coming. Here's How They Could Reshape Surveillance as We Know It*, L.A. TIMES (May 12, 2020), https://www.latimes.com/opinion/story/2020-05-12/coronavirus-tracing-app-apple-google.

[166] For example, the Facebook and Cambridge Analytica scandal was caused by a rogue third-party app exceeding the terms.

[167] Opinion, Woodrow Hartzog, *Op-Ed: Coronavirus Tracing Apps Are Coming. Here's How They Could Reshape Surveillance as We Know It*, L.A. TIMES (May 12, 2020), https://www.latimes.com/opinion/story/2020-05-12/coronavirus-tracing-app-apple-google.

[168] Susan Landau, Christy E. Lopez & Laura Moy, *The Importance of Equity in Contact Tracing*, LAWFARE (May 1, 2020), https://www.lawfareblog.com/importance-equity-contact-tracing.

[169] Susan Landau, Christy E. Lopez & Laura Moy, *The Importance of Equity in Contact Tracing*, LAWFARE (May 1, 2020), https://www.lawfareblog.com/importance-equity-contact-tracing.

[170] Susan Landau, Christy E. Lopez & Laura Moy, *The Importance of Equity in Contact Tracing*, LAWFARE (May 1, 2020), https://www.lawfareblog.com/importance-equity-contact-tracing

[171] Lucy Simko et al., COVID-19 Contact Tracing and Privacy: Studying Opinion and

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

4. Legal and Regulatory Interventions for Contact-Tracing Programs

First, we must accept that we are wading in uncharted waters with digital contact-tracing applications launched at national or global scale. It is likely that we will not know what was the best solution until much later, with the precise view that only hindsight can provide. With that in mind, because the need is so dire, and the risks of not pushing forth with a full-fledged approach are hundreds of thousands to millions of deaths, there is no choice but to throw everything at the problem and see what sticks.[172] Digital contact-tracing applications will not be enough (likely due to low user adoption), but they can theoretically help supplement or inform human contact tracing. If nothing else, it is helpful to evaluate their use in this pandemic to better prepare for the next global health crisis.

If we are to use or even try digital contact tracing, it is key that policymakers and other authorities understand the technical details of these apps, particularly the tradeoffs between centralized and decentralized digital contact-tracing proposals. This will require consultation with technical experts, as the relative dearth of technical experts embedded in government and policymaking roles is a longstanding problem.

None of these applications can be perfectly precise and without flaws, including false positives (e.g., people whose devices were in close Bluetooth proximity but who were physically not with their devices, for example[173]) and false negatives[174] (e.g., any single person not using the app). However, it appears that decentralized apps are likely the better choice, both because they are more privacy-preserving on a technical level and also because, due to the lack of consumer faith in government privacy protection, they are the better choice in terms of privacy perception and likely user adoption.

Governments and other actors seeking to launch digital contact-tracing programs should encourage the use of decentralized contact-tracing apps that are interoperable at some level. Additionally, governments should pass laws that address the use of information collected during the contact-tracing process, including during human contact tracing, in order to protect the privacy of

---

Preferences (May 8, 2020) (unpublished manuscript), .https://seclab.cs.washington.edu/wp-content/uploads/2020/05/contact-tracing-user-privacy.pdf.

[172] Tiffany C. Li, *Give All My Data to Google and the CDC*, SLATE (Apr. 6, 2020, 9:00 AM), https://slate.com/technology/2020/04/google-cdc-data-privacy-covid19.html.

[173] Ross Anderson, *Contact Tracing in the Real World*, LIGHT BLUE TOUCHPAPER (Apr. 12, 2020), https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world.

[174] Susan Landau, *Looking Beyond Contact Tracing to Stop the Spread*, LAWFARE (Apr. 10, 2020, 8:00 AM), https://www.lawfareblog.com/looking-beyond-contact-tracing-stop-spread.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

individuals. At time of writing, a number of proposals have been raised in the United States. Regulatory agencies can also release guidance on privacy protections, both regarding enforceable mechanisms and best practices for contact-tracing programs. Similarly, those who build, implement, and run contact-tracing programs should also create and agree to industry standards, in line with what researchers have been doing with interoperability standards for decentralized contact-tracing applications. Publicizing privacy protections may aid in restoring user trust, which may then help increase use of contact-tracing programs, digital or not.

D. Novel Technologies in Healthcare

The pandemic has already changed healthcare, with effects that may last long after the world recovers. For example, there has been great growth in telemedicine and telehealth services, as many healthcare providers have closed their offices or limited in-person visits.[175] The pandemic has brought some medical uses of technology to the forefront, including telehealth and telemedicine, use of medical AI in diagnostics and research, and the use of patient-facing devices and care robots in healthcare settings.

At the same time, the unique dimensions of the pandemic have changed the use of technology in medicine. The public-health emergency has created the sudden need for a large medical and healthcare workforce, both in direct response to patients in relation to COVID-19 and associated medical issues, as well as to replace healthcare workers who may be indisposed due to exposure to the virus or becoming ill themselves. The extremely contagious nature of the virus has also made it difficult to treat patients, necessitating a limitation on physical contact between patients and healthcare professionals as well as the friends and family who would otherwise be visiting. Additionally, different groups of people may be facing disparate health struggles, including exacerbated issues of bias in medical care.[176]

1. Telehealth and Telemedicine

Two unique factors of this pandemic have led to a rise in telehealth, telemedicine, and teletherapy services. First, the novel coronavirus is highly

---

[175] Kathleen T. Jordan, *An Unexpected Benefit of the Pandemic: The Doctor Will Virtually See You Now*, WASH. POST (Apr. 14, 2020, 9:17 AM EDT), https://www.washingtonpost.com/outlook/2020/04/14/telemedicine-virtual-health-coronavirus.

[176] John Eligon & Audra D. S. Burch, *Questions of Bias in Covid-19 Treatment Add to the Mourning for Black Families*, N.Y. TIMES (May 10, 2020), https://www.nytimes.com/2020/05/10/us/coronavirus-african-americans-bias.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

contagious, necessitating social distancing. Traditional physical locations where healthcare is provided have been shut down, and in-person house calls raise concerns regarding contagion as well. Second, the failures in the health systems of many nations in being able to meet medical needs of both COVID-19 sufferers and others during this time have led to a need for more medical services. Thus, in a time when more medical services are needed, and yet medical service providers cannot physically be near patients, telehealth has become an important part of healthcare across the world.

Regulators have recognized this need, relaxing some HIPAA restrictions to allow for more medical providers to more easily offer telehealth services to patients in need.[177] It is possible that these relaxations of HIPAA may pave the way for future loosening of HIPAA and related restrictions on transmission and storage of health information. Telehealth has been beneficial to many, improving access to healthcare for people in rural areas,[178] low-income populations, disabled people, and more. However, the increased use of telehealth may disadvantage people without access to stable or strong internet or computer or mobile devices.

What is interesting is not telehealth itself, or HIPAA, but rather the speed at which HHS was willing to bend HIPAA rules in a state of public-health emergency. This speaks to the malleability of HIPPA protections—and health-privacy protections in the United States generally. While the pandemic may have been a good reason to loosen these regulations, one must wonder if the regulations so easily loosened should be restructured overall to better fit future

---

[177] *COVID-19 & HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public*

Health Emergency, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 15, 2020), https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf; *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 17, 2020), https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html; Office of Civil Rights, *COVID-19 and HIPAA: Disclosures to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities*, U.S. DEPT. HEALTH & HUM. SERVS., https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf; Office of Civil Rights, *Civil Rights, HIPAA, and the Coronavirus Disease 2019 (COVID-19)*, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 28, 2020), https://www.hhs.gov/sites/default/files/ocr-bulletin-3-28-20.pdf; Office of Civil Rights, *FAQs on Telehealth and HIPAA During the COVID-19 Nationwide Public Health Emergency*, U.S. DEPT. HEALTH & HUM. SERVS., https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf.HHS Limited HIPAA Waiver

[178] Gabby Galvin, *Expanded Telehealth Has Provided a Boost for Rural America. Will It Last?*, U.S. NEWS (May 7, 2020), https://www.usnews.com/news/healthiest-communities/articles/2020-05-07/telehealth-a-boost-for-rural-america-during-coronavirus-pandemic.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

crises. Perhaps, health-privacy regulations should allow for emergency response and for technological innovation when needed, while still protecting patient privacy. If the current regulatory scheme for health privacy does not adequately protect Americans in a public-health crisis, the law must resolve this discrepancy.

2. Medical AI for Research, Diagnostics, and Triage

Artificial intelligence and machine-learning tools have also been key components of the medical and scientific response to the pandemic. Artificial intelligence describes any form of machine intelligence designed to mimic the functionality of human intelligence. Machine learning is a process by which a machine is fed a quantity of data, from which it extrapolates certain predictions based on that data.[179]

AI is being used in medical research, to search for treatments and vaccines for the novel coronavirus. For example, researchers have adapted or implemented existing AI technology for use in medical triage for COVID-19 patients. Researchers in China and the United States reportedly developed an AI-backed tool to predict which newly infected patients would likely later develop acute respiratory disease syndrome (ARDS), a severe lung disease that kills fifty percent of patients. The idea was that this tool could then be used by hospitals running low on resources to triage their patients—e.g., giving ventilators to patients less likely to develop ARDS (and thus more likely to survive the infection).[180] Another AI system designed to help hospitals triage patients is eCART, a system used by the University of Chicago Medical Center, to predict which patients will have worse medical outcomes (e.g., which patients will need intubations).[181] A Stanford team lead by Ron Li is also evaluating an automated "Deterioration Index" to identify patients whose medical conditions will likely deteriorate.[182]

These AI-enabled tools may be useful in aiding medical staff, potentially saving time and resources. They may also lift some of the burdens from physicians and other healthcare workers who would otherwise have to make

---

[179] MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE (2018).)

[180] *AI Tool Predicts Which Coronavirus Patients Get Deadly 'Wet Lung,'* YAHOO! NEWS (Mar. 30, 2020), https://news.yahoo.com/ai-tool-predicts-coronavirus-patients-deadly-wet-lung-184124238.html.

[181] Eliza Strickland, *AI Can Help Hospitals Triage COVID-19 Patients*, IEEE SPECTRUM (Apr. 17, 2020), https://spectrum.ieee.org/the-human-os/artificial-intelligence/medical-ai/ai-can-help-hospitals-triage-covid19-patients.

[182] Eliza Strickland, *AI Can Help Hospitals Triage COVID-19 Patients*, IEEE SPECTRUM (Apr. 17, 2020), https://spectrum.ieee.org/the-human-os/artificial-intelligence/medical-ai/ai-can-help-hospitals-triage-covid19-patients.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

difficult decisions on their own that would take time from their other clinical duties. One of the most tragic phenomena of this pandemic has been that the lack of medical resources has pushed doctors to triage lifesaving equipment, making decisions on who lives or dies.[183] It is possible that having an AI-enabled tool to back up a doctor's decision could alleviate some of the burden of this ethical quagmire. Medical AI tools may be able to save time and resources for health professionals, which could mean saving lives when in a public-health crisis. However, the use of AI in medical triage is fraught with ethical issues, including concerns raised by disability advocates that people with disabilities may be at higher risk of death due to triage plans prioritizing people without disabilities.[184]

AI systems should be designed with privacy interests in mind. For example, if patient data is used to train a machine learning algorithm on predicting which patients may develop which symptoms, it is necessary that the patient data is deidentified or collected in a non-identifiable manner. The use of patient data, potentially including photographs (e.g., X-ray scans of lungs to analyze COVID-related damage[185]), also comes with privacy risks. Re-identification of data is always a risk, as well as misuse of patient data. Patients may not realize how their data is used, and, while proper informed consent is necessary before collecting patient data for use in these systems, it may be difficult to gain adequate consent for difficult-to-understand tools and data usage, particularly in emergency settings. While regulations like the 21st Century Cures Act may protect patient information used in federal research, some AI systems are built by private institutions,[186] with fewer regulations on the collection and use of data. Additionally, the critical emergency nature of an active global pandemic may

---

[183] Opinion, John Chisolm, *Doctors Will Have to Choose Who Gets Life-Saving Treatment. Here's How We'll Do It*, GUARDIAN (Apr. 1, 2020, 9:08 AM EDT), https://www.theguardian.com/commentisfree/2020/apr/01/doctors-choose-life-saving-treatment-ethical-rules; Opinion, Ezekiel J. Emanuel, James Phillips & Govind Persad, *How the Coronavirus May Force Doctors to Decide Who Can Live and Who Dies*, N.Y. TIMES (Mar. 12, 2020), https://www.nytimes.com/2020/03/12/opinion/coronavirus-hospital-shortage.html; Yascha Mounk, *The Extraordinary Decisions Facing Italian Doctors*, ATLANTIC (Mar. 11, 2020),https://www.nytimes.com/2020/03/12/opinion/coronavirus-hospital-shortage.html; https://www.theatlantic.com/ideas/archive/2020/03/who-gets-hospital-bed/607807.

[184] Mike Baker, *Whose Life is Worth Saving? In Washington State, People With Disabilities Are Afraid They Won't Make the Cut*, NY TIMES (March 23, 2020), https://www.nytimes.com/2020/03/23/us/coronavirus-washington-triage-disabled-handicapped.html.

[185] Scott Lyon, *AI tool gives doctors a new look at lungs while treating COVID-19*, PRINCETON UNIVERSITY (May 21, 2020), https://www.princeton.edu/news/2020/05/21/ai-tool-gives-doctors-new-look-lungs-treating-covid-19

[186] *See, e.g.*, Baidu, *How Baidu Is Bringing AI to the Fight Against Coronavirus*, MIT TECH. REV. (Mar. 11, 2020), https://www.technologyreview.com/2020/03/11/905366/how-baidu-is-bringing-ai-to-the-fight-against-coronavirus.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

necessitate a relaxing of some privacy-based restrictions on use of data, including in AI systems.

These AI-based tools are not without their drawbacks. Many scholars have highlighted problems with bias[187] that creep into the design and implementation of many AI systems. Medical AI systems also suffer from this problem,[188] and the consequences can be literal life or death for patients.[189] While it is understandable that healthcare providers in the middle of a public-health emergency turn to any tools that can help them maximize their time and resources and help save more lives, it is troubling that some of these tools may not have been designed with fairness and equality in mind.

Privacy is an important dimension of the algorithmic-discrimination problem. Some privacy-protective measures may actually make algorithmic discrimination worse. For example, by stripping data of some identifying characteristics (like race, gender, and so on), system designers may unknowingly use biased data or data that is not reflective of their target population. This may also make it more difficult to audit the algorithms afterward, to analyze if algorithmic discrimination occurred. It is also possible that privacy laws and regulations may limit the data available to researchers and designers of AI systems.

Algorithmic discrimination can happen at different points in an AI systems, including in the designed goals of the system, the selection of training data, the choice of parameters, and more.[190] For example, an AI-based tool that predicts the likelihood a COVID-19 patient will survive intubation could rely on past data of patients that have had the virus and either did end up surviving

---

[187] *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACHINE LEARNING RES. 1 (2018); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. WASH.L. REV. REV.1, 4 (2014); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REVREV. 93, 101 (2014).)

[188] Danton S. Char, Nigam H. Shah & David Magnus, *Implementing Machine Learning in Health Care—Addressing Ethical Challenges*, 378 NEW ENG. J. MED. 981 (2018); W., William Nicholson Price II, *Medical AI and Contextual Bias*, 33 HARV. J.L. & TECH. 66 (2019); Carolyn Y. Johnson, *Racial Bias in a Medical Algorithm Favors White Patients Over Sicker Black Patients*, WASH. POST (Oct. 24, 2019, 2:00 PM EDT), https://www.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients.

[189]Gina Kolata, *Many Medical Decision Tools Disadvantage Black Patients*, NY TIMES (June 17, 2020), https://www.nytimes.com/2020/06/17/health/many-medical-decision-tools-disadvantage-black-patients.html.

[190] *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016); Joshua A. Kroll et al.,. *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017)..

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

intubation or didn't. However, the data set of patient outcomes might not include confounding factors, including race, gender, socioeconomic class, and more. The dataset may reflect biases.

For example, consider a hospital that decides to use an AI triage system that predicts patient survival based on a data set of past patients and intubation survival rates. The hospital uses this system to decide which patients are given priority when allocating ventilators. A system based on past survival data may seem unbiased and neutral. However, there are a number of ways bias could creep in. Perhaps patients living in low-income areas tended to also suffer from lack of access to consistent healthcare and nutrition, leading to worse health outcomes when hospitalized. The predictive algorithm, then, might predict outcomes that reflect those biases, predicting that low-income patients would be less likely to survive intubation. This would create what many would agree would be a discriminatory outcome: the AI tool would suggest disproportionately that low-income patients should not be prioritized. A hospital using this system would then unintentionally prioritize wealthier patients, leading to a death disparity.

Of course, human healthcare providers may also not be without their own biases. Studies have shown that some groups suffer worse outcomes than others, due possibly to the bias of healthcare workers.[191] For example, a review of pain management in hospitals found that Black and Hispanic patients were less likely to receive pain-relieving analgesia for the management of acute pain, implying that healthcare providers had made decisions based on patients' race and not on the patients' actual need for pain relief.[192] Bias may also be playing a role in creating disproportionate medical consequences for some communities in the pandemic.[193]

The law has not comprehensively addressed the risks of medical AI.[194] While

---

[191] *See, e.g.*, DAYNA BOWEN MATTHEW, JUST MEDICINE: A CURE FOR RACIAL INEQUALITY IN AMERICAN HEALTHCARE (2015); Leonard E. Egede, *Race, Ethnicity, Culture, and Disparities in Health Care*, 21 J. GEN. INTERNAL MED. 667 (2006).https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1924616/;

[192] Paulyne Lee et al., *Racial and Ethnic Disparities in the Management of Acute Pain in US Emergency Departments: Meta-Analysis and Systematic Review*, 37 AM. J. EMERGENCY MED. 1770 (2019).

[193] Opinion, Ben Crump, *For Black Americans, Bias Seen in Coronavirus Response Is Continuation of Injustice*, USA TODAY (Apr. 9, 2020, 6:39 PM), https://www.nytimes.com/2020/05/10/us/coronavirus-african-americans-bias.html; https://www.usatoday.com/story/opinion/policing/2020/04/09/black-americans-coronavirus-response-continuation-injustice/5120999002; John Eligon & Audra D. S. Burch, *Questions of Bias in Covid-19 Treatment Add to the Mourning for Black Families*, N.Y. TIMES (May 10, 2020), https://www.nytimes.com/2020/05/10/us/coronavirus-african-americans-bias.html.

[194] Jane R. Yakowitz Bambauer, *Dr. Robot*, 51 UC DAVIS L.Law REV. 383 (2017); Charlotte

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

medical AI tools can be useful in a public-health emergency like the coronavirus pandemic, the law must balance protection of patient privacy and algorithmic rights versus the need for researchers and healthcare providers to act and innovate nimbly in times of crisis.

3. Healthcare Robots

One of the myriad difficulties of healthcare in the middle of a highly contagious viral epidemic is the need to isolate patients from each other, from healthcare professionals, and from their family and friends. Some hospitals have also turned to robots[195] to assist, especially where it would be difficult or costly to have humans performing the same tasks.[196] For example, robots have been used in hospitals around the world to remotely take temperature readings,[197] a task that would otherwise require a human healthcare provider to get in close physical proximity to the patient. While the coronavirus pandemic created new needs for robots deployed in healthcare settings, robots have been frequently deployed in other disaster and emergency settings.[198] Robots can be helpful in emergency situations where a human presence would be dangerous or inefficient, including in healthcare emergencies where human proximity is a

---

Tschider, *Deus ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future*, 5 SAVANNAH L. REV. 177 (2018).

[195] Mary Meisenzahl, *An Indian Hospital Is Using Robots with Thermal Cameras to Screen Coronavirus Patients—Here's How They Work*, BUS. INSIDER (May 9, 2020, 7:45 AM), https://www.businessinsider.com/india-coronavirus-robot-uses-thermal-camera-to-take-temperature-2020-5; Robin R. Murphy et al., *Robots Are Playing Many Roles in the Coronavirus Crisis—And Offering Lessons for Future Disasters*, CONVERSATION (Apr. 22, 2020, 7:46 AM EDT), https://theconversation.com/robots-are-playing-many-roles-in-the-coronavirus-crisis-and-offering-lessons-for-future-disasters-135527; Cat Wise, *How Robots and Other Tech Can Make the Fight Against Coronavirus Safer*, PBS (May 4, 2020), https://www.pbs.org/newshour/science/how-robots-and-other-tech-can-make-the-fight-against-coronavirus-safer.

[196] Robin R. Murphy et al., *Robots Are Playing Many Roles in the Coronavirus Crisis—And Offering Lessons for Future Disasters*, CONVERSATION (Apr. 22, 2020, 7:46 AM EDT), https://theconversation.com/robots-are-playing-many-roles-in-the-coronavirus-crisis-and-offering-lessons-for-future-disasters-135527 ("One important lesson is that during a disaster robots do not replace people. They either perform tasks that a person could not do or do safely, or take on tasks that free up responders to handle the increased workload.").

[197] Mary Meisenzahl, *An Indian Hospital Is Using Robots with Thermal Cameras to Screen Coronavirus Patients—Here's How They Work*, BUS. INSIDER (May 9, 2020, 7:45 AM), https://www.businessinsider.com/india-coronavirus-robot-uses-thermal-camera-to-take-temperature-2020-5; *SNUH Uses New Methods to Prevent COVID-19 Infection*, SNUH (Mar. 26, 2020).; http://www.snuh.org/global/en/about/newsView.do?bbs_no=5113.

[198] ROBIN R. MURPHY, DISASTER ROBOTICS (2014); *International Cooperation in Deploying Robots for Disasters: Lessons for the Future from the Great East Japan Earthquake*, 32 J. ROBOTICS SOC'Y JAPAN 104 (2014)https://www.jstage.jst.go.jp/article/jrsj/32/2/32_32_104/_article; Robin R. Murphy et al., *Mobile Robots in Mine Rescue and Recovery*, 16 IEEE ROBOTICS & AUTOMATION MAG. 91 (2009).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

potential vector for deadly viruses.

Robotics scholar Robin R. Murphy and the Robotics for Infectious Diseases team she chairs have been tracking the way robots have been used during the COVID-19 response worldwide.[199] As of April 2020, Murphy's team has reported many reported uses of robots in healthcare settings or functions as part of COVID-19 response. These uses have included: disinfecting physical spaces (e.g., clinics and hospitals); telepresence abilities for healthcare workers (e.g., allowing a nurse to check on patient symptoms virtually); patient intake and visitors; patient and family socializing; delivery and dispensing of food, prescriptions, or other items; as well as testing (e.g., temperature scans).[200] As Murphy and her colleagues predict, the use of robots in COVID-19 response may lead to an increased use of robots in healthcare or other settings, as well as the development of new robots.[201]

The use of robots in healthcare settings for pandemic response raises interesting legal questions. Ryan Calo has written extensively on the "exceptional" nature of robots and the necessity for transforming laws to adapt to the needs of regulating robots,[202] including in the realm of privacy law.[203] Calo notes three unique characteristics of robots that will require transformations in law: embodiment (i.e., physical presence), emergence (e.g., the potential for autonomous, independent action), and social valence (here, the idea that robots "*feel* different to us, more like living agents").[204] Other scholars have also noted the distinctive privacy-regulation challenges stemming from these factors.[205]

---

[199] Evan Ackerman, *New Consortium Mobilizes Roboticists to Help With COVID-19 and Future Crises*, IEEE SPECTRUM (Apr. 22, 2020), https://spectrum.ieee.org/automaton/robotics/medical-robots/robotics-for-infectious-diseases-consortium; *How Robots Are Being Used for COVID-19*, ROBOTICS FOR INFECTIOUS DISEASES, https://roboticsforinfectiousdiseases.org/how-robots-are-being-used.html; Cat Wise, *How Robots and Other Tech Can Make the Fight Against Coronavirus Safer*, PBS (May 4, 2020), https://www.pbs.org/newshour/science/how-robots-and-other-tech-can-make-the-fight-against-coronavirus-safer.

[200] *See* sources cited *supra* note 199. Id.

[201] Robin R. Murphy et al., *Robots Are Playing Many Roles in the Coronavirus Crisis—And Offering Lessons for Future Disasters*, CONVERSATION (Apr. 22, 2020, 7:46 AM EDT), https://theconversation.com/robots-are-playing-many-roles-in-the-coronavirus-crisis-and-offering-lessons-for-future-disasters-135527.

[202] ROBOT LAW (Ryan Calo, A. Michael Froomkin & Ian Kerr eds., 2016); Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513 (2015).);

[203] Ryan Calo, *Robots and Privacy*, *in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS (ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS, Patrick Lin, George Bekey & Keith Abney eds., 2011).

[204] Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513 (2015).

[205] For a scoping study of literature on the field, see Christoph: Lutz et al.,, *The Privacy Implications of Social Robots: Scoping Review and Expert Interviews*, MOBILE MEDIA & COMM. 412 (2019).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

While truly autonomous robots that are capable of acting without a "human in the loop" are still a long way off, the physical embodiment of robots in healthcare settings and in emergency response creates interesting challenges for regulating these uses of robots. The types of robots used in healthcare and emergency response contexts are, as Eduard Fosch Villaronga puts it, "complex cyber-physical systems."[206] To regulate their use, the law must address the privacy implications of both digital data collection and use as well as the privacy harms specifically created by the physical presence of robots, their movements, and their physical functions. As Lutz et al. describe, "[t]he dimension of *physical privacy* is affected by the physical nature and mobility of social robots, while social robots' data collection and processing capacities affect users' *informational privacy*."[207] While technologies like medical AI and telemedicine platforms may affect a person's informational privacy, healthcare robots used in pandemic response may affect both informational privacy and physical privacy.

Additionally, the privacy impacts of robots will be influenced by the social valence of robots and our natural inclination to anthropomorphize certain robots, ascribing to them characteristics and perhaps legal protections we ordinarily would give to human beings.[208] Many healthcare robots would likely be designed as social robots, a category Kate Darling has defined as a robot that is a "physically embodied, autonomous agent that communications and interacts with humans on a social level,"[209] often "communicat[ing] through social cues, display[ing] adaptive learning behavior, and mimic[ing] various emotional states."[210] Humans often display empathy toward social robots. One study showed that humans were more likely to hesitate to strike a robot if the robot had first been given a lifelike story, suggesting that stories may influence the empathic responses of humans to robots.[211] In a healthcare setting, particularly in a dire emergency healthcare setting, humans may quickly link certain robots with emotional stories or characteristics. For example, a healthcare robot that regularly delivers pain-relieving medication to a coronavirus patient may become

---

206 EDWARD FOSCH-VILLARONGA, ROBOTS, HEALTHCARE, AND THE LAW (2019).

207 Christoph Lutz et al., *The Privacy Implications of Social Robots: Scoping Review and Expert Interviews*, 7 MOBILE MEDIA & COMM. 412 (2019).

208 Brian R. Duffy, *Anthropomorphism and the Social Robot*social robot, 42 ROBOTICS & AUTONOMOUS SYS. 179 (2003).

209 Kate Darling, *Extending Legal Protection to Social Robots: The Effects of Anthropomorphism, Empathy, and Violent Behavior Towards Robotic Objects*, *in* ROBOT LAW (Ryan Calo, A. Michael Froomkin & Ian Kerr eds., 2016).

210 Kate Darling, *Extending Legal Protection to Social Robots: The Effects of Anthropomorphism, Empathy, and Violent Behavior Towards Robotic Objects*, *in* ROBOT LAW (Ryan Calo, A. Michael Froomkin & Ian Kerr eds., 2016) ; CYNTHIA L. BREAZEAL, DESIGNING SOCIABLE ROBOTS (2002).

211 Kate Darling et al., *Empathic Concern and the Effect of Stories in Human-Robot Interaction*, 24 PROC. IEEE INT'L WORKSHOP ON ROBOT & HUM. COMM. (RO-MAN) 770 (),2015)..

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

associated with positive thoughts.

Both the emotionally intensive experience of being in a critical healthcare space (for patients, loved ones, and healthcare workers) as well as the emotionally intensive experience of living through a global pandemic may contribute to healthcare robots being associated with emotions, stories, or other human-like characteristics. This increased anthropomorphization of healthcare robots in a pandemic may have impacts on privacy, as would the increased emotional connections people may develop with the robots that function in this space and time. For example, it's possible people may experience greater privacy loss, viewing the robot's intrusions (physical or otherwise) as similar to that of a human's. It is also possible that individuals voluntarily give more data to robots (for example, answering questions about symptoms), based on feeling an emotional or quasi-human connection. On the other hand, it is also possible that individuals feel less privacy impact, particularly if, as some believe, privacy is most importantly considered a right to be let alone from the eyes of other humans.[212]

Protecting the privacy rights of individuals dealing with healthcare robots during a pandemic can be difficult, as many individuals do not understand how robots work in practice and how the use of any particular robot may impact their privacy.[213] In fact, some have argued that notice and consent is not possible with many types of robots used in healthcare, given the lack of information, amount of new knowledge needed for many users, and the resulting difficulty of obtaining truly informed consent.[214]

People who are ill may have less ability to advocate for themselves and protect themselves from privacy violations due to the use of robots. Studies have shown that women, people of color, disabled people, and other people from marginalized backgrounds already suffer disproportionately negative outcomes in healthcare, including simply not having their cares addressed by healthcare workers.[215] These people may be less able to advocate for themselves

---

[212] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[213] Christoph Lutz et al.,, *RoboCode-Ethicist: Privacy-Friendly Robots, an Ethical Responsibility of Engineers?*, PROC. ACM WEB SCI. CONF. 1 Conference.; Min Kyung Lee et al., *Understanding Users' Perception*users' *of Privacy in Human–Robot Interaction*, 6 human–robot interaction. PROC. INT'L CONF.Conference ON HUM.—ROBOT INTERACTION 181 (2011).

[214] Heather Draper & Tom Sorell, *Ethical Values and Social Care Robots for Older People*, 19 ETHICS & INFO. TECH. 49 (2017); Margot E.; Kaminski, *Regulating Real-World Surveillance*, 113 WASH. L. REV. Review 1113 (2015).

[215] *See, e.g.*, Kelly M. Hoffman et al., *Racial Bias in Pain Assessment and Treatment Recommendations, and False Beliefs About Biological Differences Between Blacks and Whites*, 113 PROC. NAT'L ACAD. SCI. U.S. 4296 (2016),

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

if they view the use of robots to be intrusive. (Though it is also possible that healthcare robots may actually create greater equity in healthcare, depending on one's perception of the comparative biases of robots and humans in providing equal care.) An additional dimension of healthcare in pandemic is the isolated nature of patients, who are unable to have friends or family visit them and act as patient advocates. If a coronavirus patient cannot muster the strength to ask for a robot to be removed, there may be no one around them who can advocate for them.

The privacy of people dealing with healthcare robots is particularly important in an emotionally fraught time like a pandemic, especially in situations where human lives are on the line. The physical presence of a robot may feel more intrusive to someone in a heightened emotional state, or possibly, the presence of a robot may be welcome, given the lack of other human contact. A person's expectation of and understanding of privacy in relation to robots will likely change in this time and setting.

While it may be tempting to argue for laws regulating the use of robots, as a category, the very different types of robots that are currently used and the different settings in which they are used require specific regulation. Particularly in sensitive contexts like healthcare, regulation of robots must happen in specific forms, with attention paid to each particular sector and type of use.[216]

II. TECH AND PRIVACY IN PANDEMIC

The COVID-19 virus is fast-moving, highly contagious, deadly, and often invisible. These factors have led to increased use of technologies allowing for the replacement of some in-person human contact in government and corporate functions. Additionally, the need to protect against the spread of the disease has led to increased use of technologies, sometimes in novel ways. Finally, social isolation and the shutdowns of many public and private spaces has led to an increased use of technologies allowing people to connect to each other, socially as well as for employment and education.

Government surveillance, be it for national security, intelligence, law enforcement, or pandemic response purposes, is important to understand and

---

http://www.nejm.org/doi/full/10.1056/NEJM200008243430809; Elizabeth G. Nabel, *Coronary Heart Disease in Women—An Ounce of Prevention*, 343 NEW ENG. J. MED. 572 (2000); Rachel Rettner, *Women Feel Pain More Intensely Than Men Do*, SCI. AM. (Jan. 23, 2012), https://www.scientificamerican.com/article/women-feel-pain-more-intensely./

[216] Eduard Fosch Villaronga et al., *Did I Tell You My New Therapist is a Robot? Ethical, Legal, and Societal Issues of Healthcare and Therapeutic Robots* (Oct. 17, 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3267832.).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

important to limit, in the interest of protecting individual freedom from government overreach. However, in the age of surveillance capitalism,[217] surveillance by other actors has emerged as an equally important phenomenon to study for privacy impacts. While employers, consumer-facing corporations, and education providers have used technology in different ways during the pandemic, it can be useful to understand this class of surveillance as distinct from government surveillance conducted under traditional surveillance powers and through traditional surveillance means. The following is a non-exhaustive exploration of different ways the pandemic has changed privacy and technology in these sectors: government, employment, education, and consumer technology.

A. Government Surveillance

Governments worldwide have proposed different surveillance initiatives dedicated to pandemic response. These include testing and contact tracing, the use of new technologies, like facial recognition and drones, as well as increased video and other forms of surveillance (including to enforce such measures as social distancing and mask wearing[218]). The privacy risks of facial recognition and drones[219] have been much studied, as has been the rise of government surveillance generally and correspondent harms to privacy. Robots have also been deployed as part of government COVID-19 response, including for monitoring, crowd dispersal, enforcing social distancing, identifying infected people, and giving public information.[220]

The technologies are not new. (For example, one could easily draw a line between the use of heat-sensing surveillance in *Kyllo v. United States*[221] to the use of heat-sensing robots in COVID-19 surveillance today.[222]) What has changed is the use of the public-health rationale behind deploying these technologies at a greater scale, and in more intrusive fashion. Government surveillance has used technological tools, but this is perhaps the first time many of these tools have

---

[217] SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2018).

[218] Jared Newman, *Smart Cameras Will Soon Check if You're Social Distancing and Wearing a Mask*, FAST CO. (May 13, 2020), https://www.fastcompany.com/90503911/smart-cameras-will-soon-check-if-youre-social-distancing-and-wearing-a-mask.

[219] M. Ryan Calo, *The Drone As Privacy* Catalyst, 64 STAN. L. REV. ONLINE 29 (2011); Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF L. REV. CIRCUIT 57 (2013).

[220] *How Robots Are Being Used for COVID-19*, ROBOTICS FOR INFECTIOUS DISEASES, https://roboticsforinfectiousdiseases.org/how-robots-are-being-used.html.

[221] 533 U.S. 27, 38 (2001).)

[222] David Yaffe-Bellany, *'Thermometer Guns' on Coronavirus Front Lines Are 'Notoriously Not Accurate,'* N.Y. TIMES (Feb. 14, 2020), https://www.nytimes.com/2020/02/14/business/coronavirus-temperature-sensor-guns.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

been used at a large scale, specifically for the stated purpose of protecting public health.

Public health as rationale for privacy invasion is relatively new for many of the technologies under discussion, though public safety has long been a fallback excuse for any number of civil-liberties violations. Public health has also been used as an excuse for violating privacy and civil rights in the past, including the institutionalization of Mary Mallon, a poor woman believed to have infected dozens of people with typhoid fever, including after she was publicly sanctioned against doing so.[223] Mallon, an asymptomatic typhoid carrier, was forcibly quarantined twice and repeatedly subjected to unwanted medical tests. She became the subject of public ridicule and died alone in forced isolation. Public health can be an excuse governments use for any number of wrongs, and laws should take care to prevent such harms. What is different now is specifically the use of the public-health rationale for government surveillance using data-driven, connected, and autonomous technologies.

It is important to note that the privacy-invasive programs that have been used elsewhere have also been used as pandemic response, with public health taking the place of other purposes, like public safety, controlling extremism, and so on. For example, U.S. government agencies have considered or have adopted contracts with Clearview AI[224] and Palantir[225] for pandemic response. Clearview AI is the embattled facial-recognition company that scraped millions of photographs from social media to develop a shadowy facial-recognition system it then sold to both governments and corporations,[226] potentially including countries like Saudi Arabia that are not particularly known for protecting human rights.[227] Previously, law-enforcement agencies across America had been relying

---

[223] Filio Marineli et al., *Mary Mallon (1869-1938) and the History Of Typhoid Fever*, 26 ANNALS GASTROENTEROLOGY 132 (2013). s

[224] *Controversial Tech Company Pitches Facial Recognition to Track COVID-19*, NBC NEWS (Apr. 27, 2020), https://www.nbcnews.com/now/video/controversial-tech-company-pitches-facial-recognition-to-track-covid-19-82638917537. This led to a response letter from Senator Ed Markey. *See* Carrie Mihalcik, *Senator Questions Clearview AI Over Coronavirus Tracking Plans*, CNET (May 1, 2020), https://www.cnet.com/news/senator-questions-clearview-ai-over-coronavirus-tracking-plans.

[225] Nick Statt, *Peter Thiel's Controversial Palantir Is Helping Build a Coronavirus Tracking Tool for the Trump Admin*, VERGE (Apr. 21, 2020, 8:36 PM EDT), https://www.theverge.com/2020/4/21/21230453/palantir-coronavirus-trump-contract-peter-thiel-tracking-hhs-protect-now.

[226] 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.

[227] Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

on public safety and criminal justice as the primary rationales for implementing facial-recognition surveillance, as well as related technological developments, like drones, robots, and algorithmic processing.[228] Many of these surveillance tactics are not new, but the new and increased uses of government surveillance during the pandemic merits attention.

Government surveillance in a pandemic raises interesting concerns for privacy. First, future privacy legislation should take note of the public-health rationale for privacy-invasive technologies and protect against abuse of that moral justification. Second, more attention should be paid to the portability of data collected for one crisis response and used in another. Or, more generally, the law should address the current lack of strict purpose limitation in collection of data and transfer to, access by, and use by government.

Further, potentially invasive programs should be undertaken only if they can be developed in privacy-preserving ways, and only if they can be shown to be actually effective from a practical, technical standpoint. It is too easy to allow for unchecked use of surveillance technologies that have no link to actual improvements in public health, leading to both a degradation in privacy and civil-liberties norms as well as a loss of faith on the part of the public in their governmental institutions.

Finally, it is likely that future crises will allow governments to exploit public health, public safety, or other rationales to justify increasing amounts of surveillance and use of privacy-invasive technologies.[229] It will be difficult to limit the onward sharing and downstream harms of data collected during these crises. Thus, future privacy legislation should create protections for downstream, distributed harms. This could include shifting to a data-protection framework, with rights including the right to request deletion, as well as algorithmic-accountability rights, including the right to contest results of an algorithmically derived decision. Additionally, the law must solve for the compound privacy harms raised by data aggregators, as we have seen commercial data aggregators sell or share data to be added to government surveillance programs.

---

enforcement.

[228] Joseph Marks, *The Cybersecurity 202: Privacy Experts Fear a Boom in Coronavirus Surveillance*, WASH. POST (Apr. 14, 2020), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/14/the-cybersecurity-202-privacy-experts-fear-a-boom-in-coronavirus-surveillance/5e94901988e0fa101a7615be.

[229] *See* Bert-Jaap Koops, *The Concept of Function Creep*, 13 Law, Innovation and Technology 1 (2021).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

B. Employer Surveillance

Similar to what we have seen with government surveillance, the technology used in corporate-employer surveillance is mostly not entirely novel or constructed out of whole cloth for the pandemic. Employers have used new technologies to track their employees in many forms for years,[230] and scholars have called for greater protections of employee privacy, particularly in the time of digital technologies that make surveillance simple.[231] However, what has changed are: (1) the scale at which employers have used these technologies to track employees; and (2) the use of a public-health rationale to justify employee monitoring.

1. Remote Work Surveillance

One of the most widely practiced methods of pandemic response has been for governments to encourage their residents to practice social distancing, while shutting down many businesses and public and private spaces. Social distancing in this context describes measures taken to maintain physical distance between humans, with the goal of preventing spread of disease.[232] Many states and municipalities in the United States enforced orders that shut down non-essential businesses, defined differently in each location.

For many white-collar workers, the pandemic has resulted in a switch to working from home, using remote technologies. An early MIT study found that an estimated 34.1% of Americans were working remotely from home by early April 2020.[233] Work from home has been a form of pandemic response. For example, one factor possibly aiding Seattle's public-health response was early partnership with local technology companies in shifting much of their workforce to remote.[234] In contrast, some workplaces have remained open and functioning,

---

[230] Steve Lohr, *Unblinking Eyes Track Employees*, N.Y. TIMES (June 21, 2014), https://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html; Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It.)*, N.Y. TIMES (Feb. 1, 2018),https://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html; https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.

[231] Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIFCal. L. REV. 735 (2017).

[232] Kaitlyn Tiffany, *The Dos and Don'ts of 'Social Distancing,'* ATLANTIC (Mar. 12, 2020), https://www.theatlantic.com/family/archive/2020/03/coronavirus-what-does-social-distancing-mean/607927.

[233] Erik Brynjolfsson et al., *COVID-19 and Remote Work: An Early Look at US Data* (Apr. 8, 2020) (unpublished manuscript), https://john-joseph-horton.com/papers/remote_work.pdf.

[234] Mary Harris, *What Seattle Did Right, and Where New York Went Wrong*, SLATE (May 1,

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

utilizing new privacy-invasive programs in a purported attempt to safeguard employees and consumers from the virus.

Workers working from home have relied on technologies, including distributed work software and services like Microsoft SharePoint and Dropbox. Many of these technologies come with their own privacy risks, from the ever-present risk of data breach to the risks of companies selling or sharing behavioral and user data to data brokers or other parties for use in marketing or other purposes users would not appreciate.

Additionally, some employers have implemented privacy-invasive software choices, including requiring employees to keep cameras on through all working hours,[235] as well as using software that tracks every single thing employees are doing on their computers during the workday (including browser search terms and email text).[236] Companies that provide employee-monitoring services, including ActivTrak, Time Doctor, Hubstaff, Interguard, and Teramind, reported huge increases in customer base and revenue, as told to the Washington Post.[237] Some have called this range of technologies "tattleware."[238]

In lieu of in-person meetings, many have turned to using teleconferencing and videoconferencing solutions, including Zoom, Microsoft Teams[239], Google

---

2020), https://slate.com/technology/2020/05/coronavirus-covid19-seattle-new-york-responses.html.

[235] Drew Harwell, *Managers Turn to Surveillance Software, Always-On Webcams to Ensure Employees Are (Really) Working From Home*, WASH. POST (Apr. 30, 2020, 10:24 AM EDT), https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance.

[236] Drew Harwell, *Managers Turn to Surveillance Software, Always-On Webcams to Ensure Employees Are (Really) Working From Home*, WASH. POST (Apr. 30, 2020, 10:24 AM EDT), https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance; Adam Satariano, *How My Boss Monitors Me While I Work From Home*, N.Y. TIMES (May 6, 2020),; https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html.

[237] Drew Harwell, *Managers Turn to Surveillance Software, Always-On Webcams to Ensure Employees Are (Really) Working From Home*, WASH. POST (Apr. 30, 2020, 10:24 AM EDT), https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance.

[238] Drew Harwell, *Managers Turn to Surveillance Software, Always-On Webcams to Ensure Employees Are (Really) Working From Home*, WASH. POST (Apr. 30, 2020, 10:24 AM EDT), https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance.

[239] Mark Hachman, *Microsoft's Solution for COVID-19 Is a Free Teams Subscription for Six Months*, PCWORLD (Mar. 4, 2020 3:45 PM PST), https://www.pcworld.com/article/3530374/microsofts-solution-for-covid-19-is-a-free-teams-subscription-for-six-months.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Hangout[240], WebEx[241], and more.[242] Many of these technologies came with their own privacy problems. Zoom in particular gained an early lead as the videoconferencing software of choice for many, leading to increased scrutiny from privacy and security advocates and researchers[243] , as well as legal and regulatory inquiry.[244] While these companies should have done better in terms of privacy, it is to some extent understandable why they failed. As a matter of scale, it is likely these companies were not prepared to deal with a sudden large-scale increase in users as well as a shift in their user base, from primarily enterprise users to the general public at large. However, regardless of reason, many of these companies failed to properly protect the privacy and security of their users, at least in the beginning of the pandemic and the large shift to work from home.

The increase use of remote working technology has also increased potential for abuse of technologies. In the unfortunate #PoorJennifer case, a person was recorded on a group Zoom chat and filmed taking their laptop into the restroom with them – and then using the toilet, while still unknowingly on camera. [245] This video was then shared on social media, without anonymization of names on the call, likely to significant harm for the individual pictured. On a more minor level, increased use of videoconferencing technology means that many will unknowingly expose information about themselves, e.g., through items in the

---

[240] Igor Bonifacic, *Google Makes Hangouts Meet Features Free in the Wake of Coronavirus*, ENGADGET (Mar. 3, 2020), https://www.engadget.com/2020-03-03-google-makes-hangouts-meet-features-free-in-the-wake-of-coronavirus.html.

[241] Jordan Novet, *Cisco Says Webex Video-Calling Service Is Seeing Record Usage Too, Even as Competitor Zoom Draws All the Attention*, CNBC (Mar. 17, 2020, 2:49 PM EDT), https://www.cnbc.com/2020/03/17/cisco-webex-sees-record-usage-during-coronavirus-expansion-like-zoom.html.

[242] Allen St. John, *It's Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.*, YAHOO! FINANCE (Apr. 30, 2020), https://finance.yahoo.com/news/not-just-zoom-google-meet-180813488.html.

[243] *See, e.g.*, Danielle Citron & Mary Anne Franks, *Cyber Civil Rights in the Time of COVID-19*, HARV. L. REV. BLOG (May 14, 2020), https://blog.harvardlawreview.org/cyber-civil-rights-in-the-time-of-covid-19; Joseph Marks, *The Cybersecurity 202: Privacy Experts Fear a Boom in Coronavirus Surveillance*, WASH. POST (Apr. 14, 2020),https://blog.harvardlawreview.org/cyber-civil-rights-in-the-time-of-covid-19/; https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/14/the-cybersecurity-202-privacy-experts-fear-a-boom-in-coronavirus-surveillance/5e94901988e0fa101a7615be.

[244] Maggie Miller, *Zoom to Expand Security, Privacy Safeguards as Part of Agreement with New York AG*, HILL (May 7, 2020, 3:48 PM EDT), https://thehill.com/policy/cybersecurity/496664-zooms-to-expand-security-privacy-safeguards-as-part-of-agreement-with.

[245] Deborah Hastings, *Zoom Blunders in the Age of COVID-19: Shirtless Lawyers, Flatulence and Naked Spouses*, INSIDE EDITION (Apr. 14, 2020, 2:19 PM PDT), https://www.insideedition.com/zoom-blunders-in-the-age-of-covid-19-shirtless-lawyers-flatulence-and-naked-spouses-59065.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

backgrounds of their home videos, or the potentially location-identifying views through their home windows. The increased use of remote working technologies that include photo, audio, or video also create greater content moderation, speech regulation, and online harassment concerns for tech platforms.[246]

On a theoretical level, some amount of privacy is lost when the social norm is for individuals to open up their private homes to view for others in a work context. This represents a fundamental shift in our understanding of public and private spaces,[247] as the office has traditionally been a semi-public space, while the home is among our most private of places.[248] The shift to remote work, aided by omnipresent monitoring and the use of video chat software, has eroded the line between office and home and changed the way people present themselves in these contexts. This shift in contextual understanding[249] may change the way we understand privacy in both work and home contexts even past the pandemic. As society's reasonable expectations of privacy shift, so too will our legal interpretation of such understandings and how the law should regulate technology and privacy.

2. In-Person Corporate Surveillance

For workers not privileged enough to work safely indoors during the pandemic, a mess of privacy problems have arisen during the pandemic. Even as the pandemic subsides, some of these in-person surveillance measures may continue, at least for a period of time. For example, we may see temperature checks or COVID-19 testing enforcement for employees as businesses return to physical office spaces.

Companies have used digital technologies to surveil employees in-person for many years.[250] For example, Amazon has been tracking employee movement through mandatory digital connected wristbands since at least 2014.[251] In

---

[246] Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. REV. 373, 392-99 (2009).

[247] Julie E. Cohen, L. *Cyberspace as/and Space*, 107." COLUM. L. REV. 210 (2007); Ari Ezra Waldman, *Safe Social Spaces*, 96 WASH. U. L. REV. 1535 (2019).

[248] Anita L. Allen, *The Declining Significance of Home: Privacy "Whilst Quiet" and of No Use to Artists or Anyone*, 4 HA: THE JOURNAL OF THE HANNAH ARENDT CENTER FOR POLITICS AND HUMANITIES AT BARD COLLEGE 84 (2016).

[249] *See* Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.

[250] Steve Lohr, *Unblinking Eyes Track Employees*, N.Y. TIMES (June 21, 2014), https://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html.

[251] Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It.)*, N.Y. TIMES (Feb. 1, 2018),

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

response to pandemic concerns, companies have also rolled out similar wearables to track employees and enforce social distancing in the workplace.[252]

Factories and warehouses have become hot spots for infection and viral transmission.[253] In response, many corporations have instituted privacy-invasive programs in an attempt to ensure the safety of their workers, products, and consumers. Some have required temperature testing before entering the workspace, surveys asking employees for symptoms, and contact tracing for any infected employees. In April 2020, the EEOC released new guidance on employer responsibilities concerning COVID-19 and ADA protections, suggesting that employers should be allowed to "administer COVID-19 testing to employees before they enter the workplace to determine if they have the virus."[254] While some employers may have also considered the use of antibody tests or immunity passports, neither type of program has emerged as a leading trend yet.

3. Digital Inequities

It is also important to note the disparate impact of digital employee surveillance on different groups. For example, women may face more negative consequences from abuse of their photos or video content recorded in remote work settings.[255] Privacy harms related to the unwanted exposure of revealing or

---

https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.

[252] Cat Zakrzewski, *The Technology 202: Buzzing Bracelets Could Become a Workplace Accessory in the Coronavirus Era*, WASH. POST (May 14, 2020), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/05/14/the-technology-202-buzzing-bracelets-could-become-a-workplace-accessory-in-the-coronavirus-era/5ebc46fd88e0fa17cddfa4c0.

[253] Caitlin Dickerson & Miriam Jordan, *South Dakota Meat Plant Is Now Country's Biggest Coronavirus Hot Spot*, N.Y. TIMES (Apr. 15, 2020), https://www.nytimes.com/2020/04/15/us/coronavirus-south-dakota-meat-plant-refugees.html, Hannah Drier, *'A Recipe For Disaster': American Prison Factories Becoming Incubators for Coronavirus*, WASH. POST (Apr. 21, 2020, 7:40 PM EDT), https://www.washingtonpost.com/national/a-recipe-for-disaster-american-prison-factories-becoming-incubators-for-coronavirus/2020/04/21/071062d2-83f3-11ea-ae26-989cfce1c7c7_story.html; Annie Palmer, *As Coronavirus Kills Another Amazon Worker, the Company's Response Is Adding to Employees' Fears*, CNBC (May 6 2020, 5:00 PM EDT), https://www.cnbc.com/2020/05/06/amazon-worker-in-illinois-dies-of-coronavirus.html.

[254] *What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws*, U.S. EQUAL EMP. OPPORTUNITY COMMISSION, https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

[255] Anita L. Allen, *Gender and Privacy in Cyberspace*, 52 STAN.L. REV. 1175 (2000); Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 392-99 (2009).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

explicit personal content, in particular, may have worse consequences for women.[256] This may be more likely to occur with greater use of remote work technologies. (Home computing devices and remote devices are likely less secure than devices routinely maintained and updated on secure office networks in the workplace.) Women, people of color, LGBT people, and other people from marginalized groups also may face greater harassment through remote work technologies, as they often face greater online harassment through communication platforms.[257] People from marginalized groups already face discrimination in the workplace,[258] so they may be less able to fight back against encroaching employer privacy invasions as well.

While white-collar workers may face digital surveillance through remote work, it is possible that some of these surveillance methods will decrease when workers return to the office. However, workers in different settings, including factories and warehouses, are unlikely to see a change, as they will continue to work in the same settings pre- and post-pandemic. These workers are also likely to have less power in fighting back against employer surveillance. Many of the people doing these jobs belong to lower income, lower education, rural, formerly incarcerated, or other marginalized groups in society. Low-income workers, contract workers, and gig-economy workers often have to face greater privacy violations in the course of business, with less power to fight against employer abuses. Effectively, pandemic-driven employer surveillance may create even greater inequalities in employee privacy, with higher-income and white-collar workers suffering fewer privacy harms for potentially shorter time periods.

Not only will people from already marginalized segments of society face greater privacy harms related to technology uses by employers in public-health emergency, but these privacy and labor harms are compounded in complex ways for those who face discrimination and disparate impacts due to more than one of their identities, creating intersectional privacy harms that are often not considered in privacy laws. Additionally, increased corporate surveillance, while worrisome for employees, may also be harmful for corporations. Individuals need privacy to be able to innovate,[259] to produce the creative insights and work

---

[256] Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014); Danielle K. Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019).

[257] Scott Skinner-Thompson, *Privacy's Double Standards*, 93 WASH. L. REV. 2051 (2018); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 L. & SOC. INQUIRY 987 (2019).

[258] Maryam Jameel & Joe Yerardi, *Workplace Discrimination Is Illegal. But Our Data Shows It's Still a Huge Problem.*, VOX (Feb. 28, 2019, 8:29 AM EST), https://www.vox.com/policy-and-politics/2019/2/28/18241973/workplace-discrimination-cpi-investigation-eeoc.

[259] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (, 2013)..

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

that corporations need to be economically successful.

Gig-economy workers will also face disparate harms, as most are considered independent contractors, without the benefits and protections given to employees.[260] The drastic fall in the economy has caused millions of Americans to lose their jobs or face cuts in job hours,[261] perhaps leading some to venture into gig-economy positions that may still be functioning as "essential" work. Instacart, a gig-economy platform that connects consumers with workers who shop and then deliver groceries and other items from stores, saw an explosion in their workforce and profits. In early May 2020, the company announced that it had recruited 300,000 new workers in a month, with plans to hire 250,000, at the same time that the company also announced it had hit its sales goals through 2022.[262]

Gig-economy or sharing companies like Instacart often already operated on an information asymmetry, profiting from the data gathered on consumers and gig-economy workers alike, with their independent-contractor workers unable to fight against privacy invasions.[263] Gig-economy workers already have few privacy protections and are often subject to surveillance and data collection and tracking from companies. Many gig-economy workers are uniquely vulnerable, as they often have difficulty finding other employment,[264] so they have less ability to fight against corporate privacy invasions. These privacy harms likely were exacerbated or at least continued at a greater scale during the pandemic. There is little incentive for these companies to increase privacy protections, particularly as they are not treating gig-economy workers as employees but rather as independent contractors. Gig-economy workers often also face some of the same vulnerabilities as blue collar workers, and depending on the job, the groups often intersect, creating intersectional harms that multiply for workers who experience overlapping forms of vulnerability in the workplace.

---

260 Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623 (2017).

261 Rachel Siegel & Andrew Van Dam, *3.8 Million Americans Sought Jobless Benefits Last Week, Extending Pandemic's Grip on the National Workforce*, WASH. POST (Apr. 30, 2020, 5:03 PM EDT), https://www.washingtonpost.com/business/2020/04/30/weekly-jobless-claims-unemployment.

262 Tyler Sonnemaker, *Instacart's Army of Shoppers Has Exploded from 180,000 to 500,000 Since the Start of the Pandemic—And Some Workers Say It's Making the Job More Difficult for Everyone*, MSN (May 8, 2020), https://www.msn.com/en-us/money/other/instacarts-army-of-shoppers-has-exploded-from-180000-to-500000-since-the-start-of-the-pandemic-and-some-workers-say-its-making-the-job-more-difficult-for-everyone/ar-BB13O564.

263 Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623 (2017).

264 Univ. Cal. - Santa Cruz, *Already Vulnerable, Gig Economy Workers in SF Suffer During Pandemic, Survey Finds*, PHYS ORG (May 5, 2020), https://phys.org/news/2020-05-vulnerable-gig-economy-workers-sf.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

4. Legal and Regulatory Interventions to Protect Employee Privacy

With employer surveillance as with government surveillance, we have not necessarily seen new technologies develop in reaction to pandemic needs. Rather, what has happened is a change in scale and rationale: greater use of existing technologies for digital surveillance; and a new justification for use of these privacy-invasive technologies. (A similar phenomenon has occurred with government surveillance, as discussed previously.) Before the pandemic, digital employee surveillance was often justified for economic and efficiency reasons.[265] Now, during the pandemic, employers are justifying digital surveillance for reasons related to public health (including the social health benefits of keeping remote coworkers connected[266]).

Scholars have called for greater legal protections for employees against corporate surveillance. Ifeoma Ajunwa, Jason Schultz, and Kate Crawford proposed three solutions: (1) an omnibus federal information-privacy law that would include employee protections; (2) a sector-specific Employee Privacy Protection Act; or (3) a more limited sector-specific and context-specific Employee Health Information Privacy Act.[267] For Ajunwa et al., "the protection of workers' privacy is a civil rights issue: both for the protection of human dignity rights and because privacy invasions can serve as vehicles for unlawful discrimination."[268] Employee health information is particularly important to protect in the midst of a public-health emergency, but generally, the privacy rights of employees are something the law should take pains to protect, given the power asymmetry between employers and employees.

It appears likely that employer surveillance will continue. If anything, the rise in employer surveillance during this pandemic will likely raise the floor for employer surveillance after the pandemic is over. Thus, it will become even more important for the law to protect employees. Lawmakers in the United States should include specific employee-centric provisions in future national privacy regulation. Additionally, laws like HIPAA and GINA can be amended to strengthen protections employees have against employer collection, use, and sharing of their health and genetic data.

---

[265] Ifeoma Ajunwa, Kate Crawford & Jason, Schultz, *Limitless Worker Surveillance*, 105 CALIF L. REV. 735 (2017).

[266] Drew Harwell, *Managers Turn to Surveillance Software, Always-On Webcams to Ensure Employees Are (Really) Working From Home*, WASH. POST (Apr. 30, 2020, 10:24 AM EDT), https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance.

[267] Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735 (2017).

[268] Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735 (2017).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

While many advocates have called for greater privacy protections of employees, employers now have new justification for digital surveillance programs. With the public-health crisis still in full swing, it is likely that public-health rationales will prove persuasive, allowing employers to expand surveillance programs. Even after the pandemic subsides, these changes in employment-surveillance norms will likely have long-term effects. Norms will shift, and societal expectations of privacy will shift, paving the way for even more employee surveillance in the future.

C. Education Privacy in Pandemic

In response to the pandemic, both public and private schools in many states and municipalities have shut down, including K-12 schools as well as higher-education settings. In early March, ABC News estimated more than 290 million students worldwide have had school disrupted due to COVID-19.[269] As schools have closed physical, in-person spaces, many have shifted to remote, online teaching. With that shift has come a natural change in relationships with privacy and technology, on the part of students, parents and guardians of younger students, educators, and education institutions.

Student privacy has long been an issue in an era of digital learning and connected tools. From the ill-fated One Laptop per Child program,[270] to positive uses of technology in the physical classroom, to innovative online-learning developments, technology has changed the way education is done in our society. Changes in society have also changed education technology. For example, the rise of wireless and broadband access to the internet, as well as the increased access to mobile devices, has allowed for education services to proliferate online, including educators teaching through YouTube, apps like Khan Academy and Duolingo, and the phenomenon of massive open online courses (MOOCs) and other "virtual learning environments,"[271] as well as free, open-knowledge resources like Wikipedia. All of these new technological innovations come with their own privacy issues. Additionally, many students have faced a loss of physical education privacy, as many have been forced to move home or stay home, losing the physical privacy a school or library may have provided.

The primary laws protecting student privacy in the United States include the

---

[269] Kelly McCarthy, *The Global Impact of Coronavirus on Education*, ABC NEWS (Mar. 6, 2020, 2:54 PM), https://abcnews.go.com/International/global-impact-coronavirus-education/story?id=69411738.

[270] MORGAN AMES, THE CHARISMA MACHINE (2019).)

[271] Elana Zeide and Helen Nissenbaum, *Learner Privacy in MOOCs and Virtual Education*, 16 THEORY AND RESEARCH IN EDUCATION 3 (2018).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Children's Online Privacy Protection Act (COPPA), which protects children's online privacy, and the Family Educational Rights and Privacy Act (FERPA), which protects student records held by public institutions. These laws generally target privacy protection to specifically protect the privacy of a class of users (children), a type of data (student records), or a setting (public educational institutions). However, these and other privacy laws do not protect a broader conception of educational privacy, which includes protection of the physical or virtual space[272] necessary for students and educators to freely engage in the pursuit of knowledge.

Julie E. Cohen has argued for privacy as a right that protects the ability for individuals to creatively explore and create their identities.[273] Neil Richards has identified the right to intellectual privacy, the privacy necessary to safeguard our intellectual thoughts and develop new ideas freely.[274] Ari Ezra Waldman has called for privacy law to protect "safe social spaces" in which "environments of information exchange in which disclosure norms are counterbalanced by norms of trust backed endogenously by design and exogenously by law."[275] Building on these concepts, we ought to understand educational privacy as a distinct privacy right that safeguards the ability for a student to safely explore ideas and knowledge, to develop their intellectual selves and their personal selves, as well as the ability for educators and researchers to facilitate and participate in intellectual endeavors in the education context. This educational privacy right should be linked to the essential purpose for education to provide social space for students to learn and grow through learning, for educators to impart knowledge and foster intellectual growth, and for researchers to produce and disseminate knowledge.

During the pandemic, privacy issues with remote learning technologies and innovations have only increased,[276] as more students and learners are pushed to take learning from the physical to digital realm. Students have lost much of their educational privacy interests, harms sometimes aided and sometimes ameliorated by use of technologies.

1. Education Technology

---

[272] Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure,* 75 U. CHI. L. REV. 181-201 (2008)

[273] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013).

[274] Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

[275] Ari Ezra Waldman, *Safe Social Spaces*, 96 Washington University L. Rev. 153 (2019).

[276] Jane Bailey et al., *Children's Privacy Is at Risk With Rapid Shifts to Online Schooling Under Coronavirus*, CONVERSATION (Apr. 21, 2020 10:08 AM EDT), https://theconversation.com/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus-135787.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Shifting education to remote, online spaces has led to an explosion in the use of education-surveillance technology, including software installed on school-sanctioned devices that can track the activity of students using the device. This category of privacy-violating technology also includes exam-proctoring software,[277] like Proctorio, a program which uses facial-detection software to monitor students taking an exam online, by tracking eye movements, background activity, and noise—all through access to the student's camera and microphone.[278] These programs can collect many forms of data from students, including photos, video recordings of students at their computers, voice data, browsing history, keystroke data, and more.[279]

The increased use and reliance on digital-education technology tools has raised concerns for privacy. Many of these programs have come under fire in the early phases of the pandemic for a wide variety of privacy and security concerns. Zoom, a remote videoconferencing application, found itself the subject of investigation by the New York Attorney General's Office for privacy concerns,[280] and the city of New York temporarily stopped use of Zoom for all public schools.[281] Some of the privacy harms from this shift to online learning could be ameliorated by focusing more attention to asynchronous learning as opposed to live sessions where students must log in and potentially have video and audio on. Asynchronous learning could also aid in lessening unequal access to education in times of public-health crisis and the effects of the digital divide.[282]

---

[277] Monica Chin, *Exam Anxiety: How Remote Test-Proctoring Is Creeping Students Out*, VERGE (Apr. 29, 2020, 8:00 AM EDT), https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education.

[278] Jake Evans, *ANU to Use Facial Detection Software on Student Computers in Response to Coronavirus Remote Exams*, ABC (Apr. 20, 2020), https://www.abc.net.au/news/2020-04-20/coronavirus-anu-to-use-ai-spying-software-on-student-computers/12164324.

[279] Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools*, 97 N.C. L. Rev. 1673 (2019).

[280] Danny Hakim & Natasha Singer, *New York Attorney General Looks Into Zoom's Privacy Practices*, N.Y. TIMES (Mar. 30, 2020), https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html; Lauren Feiner, *Zoom Strikes a Deal with NY AG Office, Closing the Inquiry Into Its Security Problems*, CNBC (May 7, 2020, 3:54 PM EDT), https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html; https://www.cnbc.com/2020/05/07/zoom-strikes-a-deal-with-ny-ag-office-closing-security-inquiry.html.

[281] Valerie Strauss, *School Districts, Including New York City's, Start Banning Zoom Because of Online Security Issues*, WASH. POST (Apr. 4, 2020, 12:31 PM EDT), https://www.washingtonpost.com/education/2020/04/04/school-districts-including-new-york-citys-start-banning-zoom-because-online-security-issues.

[282] Kelly A. Hogan & Viji Sathy, *8 Ways to Be More Inclusive in Your Zoom Teaching*, CHRON. (Apr. 8, 2020), https://www.chronicle.com/article/8-Ways-to-Be-More-Inclusive-in/248460; Hannah Natanson, L*ive vs. Tape-Delayed: How Two Approaches to Online Learning Change Life for*

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Additionally, using digital platforms for learning comes with potential for harassment and abuse. Early in the pandemic, the phenomenon known as "Zoombombing" began occurring, as people started to use Zoom as a venue for harassment and disruption.[283] A Connecticut teen was charged with computer crime for Zoombombing—in this case, entering a high school's online classes and disrupting the class with obscene language and hand gestures.[284] Harmful activity on Zoom and other online video-conferencing platforms reached a bad enough threshold that the FBI released an article[285] on guidance for defending against these attacks, and the Department of Homeland Security's Cybersecurity and Critical Infrastructure Security Agency (CISA) also published guidance on this issue.[286]

These education technologies are not new, but the scale at which they are being used is new, as most schools around the world have shut down physical campuses. It is possible that more schools will rely on distance education in the future, perhaps due to familiarity gained during the pandemic. As such, these technologies—and their impact on privacy—will become even more important in the future.

2. In-Person Campus Surveillance

As schools attempt to reopen in full or in part, a number have proposed in-person testing requirements, such as temperature scanning, COVID-19 virus

---

Teachers and Students, WASH. POST (Apr. 28, 2020, 6:34 AM EDT), https://www.washingtonpost.com/local/education/live-vs-tape-delayed-how-two-approaches-to-online-learning-change-life-for-teachers-and-students/2020/04/25/250fb7d0-7bfe-11ea-9bee-c5bf9d2e3288_story.html.

283 David Z. Morris, *Zoom Meetings Keep Getting Hacked. Here's How to Prevent 'Zoom Bombing' on Your Video Chats*, FORTUNE (Apr. 2, 2020, 2:45 PM EDT), https://fortune.com/2020/04/02/zoom-bombing-what-is-meeting-hacked-how-to-prevent-vulnerability-is-zoom-safe-video-chats; Hannah Sparks, *Trolls Crash Zoom Alcoholics Anonymous Meetings: 'Alcohol Is Soooo Good,'* N.Y. POST (Apr. 2, 2020, 11:55 AM EDT), https://nypost.com/2020/04/02/trolls-crash-zoom-aa-meetings-alcohol-is-soooo-good.

284 *Teen Arrested After 'Zoom Bombing' High School Classes*, N.Y. POST (Apr. 8, 2020, 11:55 AM EDT), https://nypost.com/2020/04/08/teen-arrested-after-zoom-bombing-high-school-classes.

285 Press Release, FBI Boston, FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic (Mar. 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

286 Press Release, Cybersecurity & Infrastructure Security Agency, FBI Releases Guidance on Defending Against VTC Hijacking and Zoom-Bombing, (Apr. 2, 2020), https://www.us-cert.gov/ncas/current-activity/2020/04/02/fbi-releases-guidance-defending-against-vtc-hijacking-and-zoom.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

testing, or possibly immunity passports or other verification.[287] The purported goals are to help recreate the benefits of having physical school spaces, including reducing the disparate impact on marginalized students who are harmed more by the shutting down of schools.

However, increased testing and data collection on campus can have a harmful impact on privacy rights for students and staff in educational institutions. First, any new collection of data will create risks of data exposure, including to hackers and bad actors. Second, testing on campus would come with the same issues related to COVID-19 testing in general, as would immunity passports or other forms of COVID-related medical verification used on campus.

What would differentiate these privacy-invasive measures from other forms of surveillance and data collection would be the educational context and the educational institution as the primary data controller and possibly the primary physical point of data collection. This narrows the field for regulation slightly, as some of the privacy harms can be stemmed solely by regulating educational instructions and educational privacy rights. Here, laws like FERPA and HIPAA may apply in only limited manners.

Increasing surveillance in-person on campus could lead to a loss in students' expectations of privacy. Students may feel like they have less privacy on campus, due to an increased surveillance apparatus present throughout the campus experience. This could lead to a loss in perceived educational privacy protections, making students less willing or able to pursue their intellectual interests and develop their knowledge and skills.

3. Digital Inequities

Distance learning has a potentially discriminatory impact on some groups. The shift to online learning exposes in even starker terms the digital divide, highlighting those who live in "digital poverty," with less or no access to the internet or computing devices.[288] An estimated 17% of students nationwide lack

---

[287] *See, e.g.*, Jenna Zibton, *Virginia Schools Preparing for a Variety of Scenarios When Students Return in the Fall*, WSLS 10 NEWS (May 13, 2020, 7:53 AM), See, e.g., https://www.wsls.com/news/local/2020/05/12/virginia-schools-preparing-for-many-scenarios-when-students-return-in-the-fall.

[288] Deborah Brown, *Closing the 'Digital Divide' Critical in COVID-19 Response*, HUM. RTS. WATCH (Mar. 25, 2020, 1:15 PM EDT), https://www.hrw.org/news/2020/03/25/closing-digital-divide-critical-covid-19-response; Dana Goldstein et al., *As School Moves Online, Many Students Stay Logged Out*, N.Y. TIMES (Apr. 6, 2020), https://www.nytimes.com/2020/04/06/us/coronavirus-schools-attendance-absent.html; Nicole Gaudiano, *Coronavirus Quarantines Could Rob Poor, Rural Students of Access to Education*,

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

access to a computer at home, and an additional 18% lack access to broadband internet at home.[289] Before the pandemic, many of these students could have taken classes in person and relied on libraries, cafes, and other spaces for access to the internet and/or computers. During the pandemic, these options evaporated, worsening the already problematic digital divide.[290]

This shift to remote education has also caused unequal privacy harms that have impacted groups in disparate ways. Privacy-invasive education surveillance systems often require access to devices and the internet, which can further exacerbate digital inequalities. Students who lack stable internet access have not been able to participate in school and related education activities now moved online. Similar problems have faced students who do not have access to their own computer or mobile device, some of whom must share limited remote-computing equipment with multiple family members. Privacy-invasive software that scans activities and files on devices will thus harm the privacy both of the student as well as anyone else using the device, creating disparate privacy harms for low-income families who share devices.

Just as the shift to remote online work has changed the boundaries between work and home, affecting the way society understands these two separate contexts and the corresponding expectations of privacy in each,[291] so has the shift to remote education changed the boundaries between school and home. Students have certain expectations of privacy in the education setting. At the very least, there is an expectation, especially among older K-12 students and higher-education students, that schools offer spaces for private exploration of ideas and identities[292] and learning without undue interference from family. For college students, this often meant an entirely separate physical surrounding, for

---

POLITICO (Mar. 10, 2020), https://www.politico.com/news/2020/03/10/coronavirus-quarantines-rural-students-125048; *Poor U.S. Students Miss Out As Virtual Learning Sharpens Divide*, MSN (Apr. 18, 2020), https://www.msn.com/en-us/news/us/poor-us-students-miss-out-as-virtual-learning-sharpens-divide/ar-BB12NEgC; Shoshana Wodinsky, *Not Everyone Can Go to School Online*, GIZMODO (Apr. 7, 2020, 4:10 PM), https://gizmodo.com/not-everyone-can-go-to-school-online-1842726588.

[289] *Million of Kids Are Struggling in School Because They Don't Have Internet Access at Home*, MARKET WATCH (June 10, 2019, 4:22 PM ET), https://www.marketwatch.com/story/nearly-3-million-students-in-the-us-struggle-to-keep-up-in-school-due-to-lack-of-home-internet-2019-06-10.

[290] Dana Goldstein et al., *As School Moves Online, Many Students Stay Logged Out*, N.Y. TIMES (Apr. 6, 2020), https://www.nytimes.com/2020/04/06/us/coronavirus-schools-attendance-absent.html.

[291] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).

[292] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

the many who lived in school dorms or on their own in college towns.

Even for those living at home, schools provided spaces where students could expect to listen to lectures with a certain sense of privacy from some parties (namely, family). On the verso, students previously had an expectation of privacy regarding the separation of their home from their schools. They could reasonably expect that they would be able to protect information about their homes from the eyes of their fellow students or educators. Students who may have been able to pursue study of subjects independent of family consideration now lose the privacy of having separate educational spaces. (Consider the closeted gay teen studying LGBT history in defiance of religious conservative parents, who now must do all research from home, on shared devices.)

With the shift to online learning, students are unable to protect the divide between their home and school spaces. Students in families facing more financial stress in this time are also at a disadvantage. Older students may be pressed to take on more work hours to make up for lost wages from other family members. Younger students may lack the parental supervision necessary for setting up and engaging in remote education. (For example, someone has to make sure to turn on the computer and connect to the online video session at the right times every day.) All of these personal financial circumstances may now be made public, or at least become visible to fellow students and educators, as the privacy-invasive nature of education technologies would expose situational factors like whether a parent was consistently able to help a younger student during class.

The increased use of remote communication technologies in education also creates disadvantages for some students, based on income and socio-economic status.[293] Consider the student living in a multigenerational household with parents, grandparents, and multiple siblings all in one small apartment, where it may be difficult to find any space quiet and isolated enough to participate fully in online classes or to do online study, even during the times the student is able to wrangle the family's single computer for use. This student might not have steady Wi-Fi access or may be defaulting to a limited mobile data plan for accessing the internet. This student would be at a profound disadvantaged compared to a classmate who had access to better technology and home support.

The pandemic has changed our society's understanding of schools and homes as spaces,[294] and has blurred the divide between school and home,

---

[293] Michele E. Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1403-04 (2012).

[294] Cohen, Jean L. "*Cyberspace as/and Space*, 107 COLUM. L. REV. 210 (2007)."; Ari Ezra

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

resulting in new understandings of what should be a reasonable expectation of privacy in either context.[295] Students learning online through video communications technologies must now allow their fellow students and teachers into the privacy of their homes, including (for some) whatever objects are in viewing distance of their computers. Students who live in physical settings without the space and quiet necessary for learning via distance education have been placed at a disadvantage. Some students may feel a sense of shame about showing photos or videos of their home environments to other students. Consider the lower-income scholarship student at a private school who must now virtually invite their wealthier peers to view their home. However, technology can also be used to help ameliorate some of these harms. For example, students have taken to using Zoom virtual backgrounds to keep their homes from public view even while on video chat.[296]

Many students will suffer disparate harms in this time of pandemic. Not only will lower income students face financial stresses with less ability to fight against privacy invasions,[297] but students who are themselves parents will face greater burdens as they attempt to navigate their studies (and sometimes work) at the same time as handling childcare. Even in households where both parents work from home, women have still been doing more childcare and more household work during the pandemic era.[298] This means a disproportionate harm to women students,[299] as they will have less time to keep up with schoolwork compared to their male peers. This sharp inequality will also be reflected in more burdens on women who must parent children as they navigate new education technologies when schools are shut down.[300] Women may be found to be less productive[301]

Waldman, *Safe Social Spaces*, 96 WASH. U. L. REV. 1535 (2019).

[295] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).

[296] Zita Fontaine, *Zoom's Virtual Backgrounds Help Fight Inequality*, MEDIUM (Apr. 12, 2020), https://medium.com/age-of-awareness/zooms-virtual-backgrounds-help-fight-inequality-624da895634e.

[297] Michele E. Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1403-04 (2012).

[298] Claire Cain Miller, *Nearly Half of Men Say They Do Most of the Home Schooling. 3 Percent of Women Agree.*, N.Y. TIMES (May 6, 2020), https://www.nytimes.com/2020/05/06/upshot/pandemic-chores-homeschooling-gender.html.

[299] Jennifer Medina & Lisa Lerer, *When Mom's Zoom Meeting Is the One That Has to Wait*, N.Y. TIMES (Apr. 22, 2020), https://www.nytimes.com/2020/04/22/us/politics/women-coronavirus-2020.html.

[300] Claire Cain Miller, *Nearly Half of Men Say They Do Most of the Home Schooling. 3 Percent of Women Agree.*, N.Y. TIMES (May 6, 2020), https://www.nytimes.com/2020/05/06/upshot/pandemic-chores-homeschooling-gender.html.

[301] Colleen Flaherty, *No Room of One's Own*, INSIDE HIGHER ED (Apr. 21, 2020), https://www.insidehighered.com/news/2020/04/21/early-journal-submission-data-suggest-

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

than their peers as both students and workers who happen to be parents of students. Women likely will bear the bulk of the burden in supporting their children in transitioning to remote learning technologies, and will likely then suffer unique and disproportionate privacy harms[302] related to the use of such technologies.[303]

Students, parents, and educators may all face disparate harms due to coronavirus epidemic as well as the push to online learning aided by new technologies. These harms may fall upon those who belong to low-income, rural, undocumented, disabled, or other groups. An additional harm may simply be that students will be pressed to disclose their conditions to educators, fellow students, and administrators during this time. For example, students with some "hidden" disabilities may be forced to ask for accommodations, if their disabilities make remote distance learning difficult.[304] This disclosure can lead to a loss of privacy and a sense of lack of control over one's own personal health information, financial information, or more.

4. Legal and Regulatory Interventions to Protect Education Privacy

a. Existing Protections Are Not Enough

The educational privacy interests of students are particularly important to safeguard in a public-health emergency. As Elana Zeide writes, students may themselves be an especially vulnerable population when it comes to privacy.[305] Many students are children, a class the law has consistently recognized as deserving of particular protections, including within U.S. privacy jurisprudence.[306] Students often have little choice regarding the educational-privacy practices of their schools.[307] As Zeide notes, FERPA and similar state laws "were designed for a world of paper records, not networked, cloud-based platforms that collect information automatically"[308]—i.e., the very platforms

covid-19-tanking-womens-research-productivity.

302 ANITA ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988).

303 DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); Anita L. Allen, *Gender and Privacy in Cyberspace*, 52 STAN. L. REV. 1175 (2000).

304 Johnathan Custodio, *Disabled Students Already Faced Learning Barriers. Then Coronavirus Forced an Abrupt Shift to Online Classes.*, CHRON. (Apr. 7, 2020), https://www.chronicle.com/article/Disabled-Students-Already/248444.

305 Elana Zeide, *Education Technology and Student Privacy*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 70-70 (Evan Selinger, Jules Polonetsky & Omer Tene eds., 2018).

306 *See* The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6505 (2018). A

307 Elana Zeide, *Education Technology and Student Privacy*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 70- (Evan Selinger, Jules Polonetsky & Omer Tene eds., 2018).

308 Elana Zeide, *Education Technology and Student Privacy*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 70- (Evan Selinger, Jules Polonetsky & Omer Tene eds., 2018).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

being utilized at great scale by educational institutions during this shift to online learning.

Only public educational institutions, or institutions that receive public funding, are subject to FERPA.[309] FERPA imposes certain obligations on public educational institutions, as well as (by proxy) institutions that receive data from them. FERPA imposes restrictions on access and transfer of student data and allows students and parents certain rights regarding student data. However, FERPA is limited to only applying to public institutions, and many schools are private. During the pandemic, most schools, public and private, transitioned to online learning. Many schools, public or private, have also relied on private education-technology companies. While the data collected and transmitted by the public institution would be protected under FERPA, public institutions may still be encouraging use of private companies' technologies, which would not necessarily be covered, depending on how data is collected from students. Zeide notes that the institutional reliance on FERPA creates undue burden for students, parents, and educators, and fails to protect the privacy of students.[310]

Second, FERPA only applies to certain educational student records and not all student data collected in the course of educational experience. For example, while student grades would be considered data covered under FERPA, photos of students taken during exam monitoring would not. Third, FERPA allows for a variety of permitted disclosures of student records, including to other organizations acting on behalf of the school for legitimate purposes. With more parties having access to student data, it is more difficult to safeguard the privacy of students. Additionally, new forms of data are being generated that may or may not be considered protectable under FERPA. (Consider, for example, screenshots of Zoom sessions that include small profile photos or live camera of students. While school photographs can be protectable under FERPA, this new class of content or data may not be.) FERPA is rather limited in scope and does rather little to protect students or their parents and guardians from the privacy impacts of the pandemic-fueled shifts in use of technology.[311]

Many education technology companies will have to comply with privacy laws and general consumer-protection laws. FTC authority would extend to companies and services like Zoom, WebEx, Google Classrooms, and exam-monitoring companies. For these education companies and platforms, the FTC

---

[309] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2018); 34 C.F.R. § 99 (2019).

[310] Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L.Law REV. 339 (2016).

[311] Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L.Law REV. 339 (2016).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

could still enforce similar privacy protections as it would in other sectors. Education technology companies thus have to adhere to similar standards as all companies regarding privacy, including posting privacy notices and (importantly) not violating any of the terms that they set out in their privacy notices or terms of service. If a company were found to have not upheld the representations they made out to consumers in their terms, the FTC would have authority to enforce judgments against them.

Additionally, for education settings involving children, additional federal and state legal protections would apply for children's privacy. The Children's Online Privacy Protection Act (COPPA) protects the privacy of children under thirteen. Under COPPA, companies must adhere to a set of standards, including posting visible privacy policies and obtaining verifiable parental consent before collecting the data of children under thirteen. Parents and guardians of children under thirteen also have special rights under COPPA, including a right to revoke consent at any time and request that a company delete their child's data. Some states also have special protections for children's privacy. For example, California's "eraser law" allows children under eighteen to request companies delete their data, among other rights.[312]

However, even with existing protections, privacy laws in the United States are insufficient to protect privacy, for consumers as students and as individuals. Private-sector privacy laws do not sufficiently protect against the harms of Big Data and the downstream harms of data that may be abused or used against a person after sale, transfer, aggregation, reidentification, or more.[313] U.S. privacy law must safeguard civil liberties against the threat of data brokers and the data economy. Individuals need a way to legally seek recourse for distributed downstream data harms, including harms compounded by biased or faulty algorithmic systems.[314] One way to do this is to create better laws addressing algorithmic harms, allowing individuals to seek redress for incorrectly made algorithmic decisions that impact fundamental rights, for example.

b. A Right to Educational Privacy

Current laws dealing with education and privacy protect privacy rights based on types of data subjects: students, consumers, and so on. However, these laws do not protect the right of an individual to have the environmental privacy necessary for pursuing a path of education. The laws do not protect the privacy provided by the physical presence of a school or education institution, or the

312 CAL. BUS. & PROF. CODE §§ 22580-22582 (West 2019).

313 Margot E. Kaminski, *Regulating Real-World Surveillance*, 113 WASH. L. REV. 1113 (2015).

314 Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

privacy provided by an educational platform that allows for individualized learning. Education privacy laws generally also do not protect the educational privacy rights of educators or researchers, who also benefit from the privacy of physical education spaces.

The use of education technologies in times of pandemic have exposed the need for an updated right to educational privacy. The increased use of new education technologies, the public-private hybrid nature of many education technology platforms, and the unique vulnerabilities of the student population give rise to the need for a new right to educational privacy, a right the law should protect in addition to protections for children and existing protections for student privacy in public institutions. Some, including Khalilah Barnes, have even called for the creation of a Students' Bill of Rights,[315] protecting key rights like privacy.

The heightened sensitivities of the pandemic era expose a number of gaps in the legal protections for students. First, there should be more legal limitations on private educational institutions collecting, using, and sharing student data. FERPA protections do not apply to most collection of student data done by private platforms. In addition to relevant privacy obligations under COPPA and general privacy laws, educational institutions (public or private) should be held to a higher standard. The law should recognize the school or the educational institution as a specific place and context, with specific privacy expectations that are different from other business contexts.

Additionally, the increased use of educational technologies has exposed the necessity of addressing the disparate harms suffered by people from various marginalized communities as a result of reliance on new technologies. New privacy laws should take care to address the special needs of different students, e.g., protecting against online harassment, which disproportionately affects some groups. Students from marginalized populations may have special needs when it comes to educational privacy, including the need to have private space—digital or offline—when private space is at a premium at home.

Laws narrowly tailored to address the space necessary for educational privacy should allow for innovation across education sectors, including private-sector educational platforms. The law should recognize the educational-privacy interests that students have in protecting the privacy of their educational paths and learning processes, to aid in independent exploration of ideas and personal

---

[315] Valerie Strauss, *Why a 'Student Privacy Bill of Rights' Is Desperately Needed*, WASH. POST (Mar. 6, 2014, 3:30 PM EST), https://www.washingtonpost.com/news/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

and educational development.[316] Protecting educational privacy as a distinct right would acknowledge that students of all ages, in public and private institutions, have a privacy interest linked specifically to the concept of education as requiring intellectual freedom.

Furthermore, educational privacy should encompass privacy protection for educators and researchers as well, as all are part of the larger knowledge production system. To protect the institution of formalized education, we should honor and protect the privacy necessary for students, educators, and researchers to teach, learn, generate, and share knowledge.

D. Consumer-Connection Technologies

Remote-communication technologies have been used to a great extent in employment and education settings in response to the changes in society caused by the pandemic. However, technologies like Zoom, Google Hangouts, and other remote-communication technologies have also been used to increased effect by ordinary human beings outside of their roles as employees or students.[317] All of these technologies come with privacy and security issues.[318] It is important to discuss the impact the pandemic has had on society's relationship with privacy and technology, on an individual, human level.

1. Remote-Connection Technologies

As the pandemic has enforced social distancing conditions, humans have turned to technologies to stay in touch and maintain social relationships. This has included use of mobile phones and connected devices to communicate, whether through text messaging, phone calls,[319] video calls, and more. In early April, Verizon reported an average of 800 million wireless calls a day during the week, more than double the number of calls usually made on Mother's Day (often one of the busiest days of the year for phone calls).[320] In the same time

316 Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

317 Taylor Lorenz et al., *We Live in Zoom Now*, N.Y. TIMES (Mar. 17, 2020), https://www.nytimes.com/2020/03/17/style/zoom-parties-coronavirus-memes.html.

318 Allen St. John, *It's Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.*, YAHOO! FINANCE (Apr. 30, 2020), https://finance.yahoo.com/news/not-just-zoom-google-meet-180813488.html.

319 Cecilia Kang, *The Humble Phone Call Has Made a Comeback*, N.Y. TIMES (Apr. 9, 2020), https://www.nytimes.com/2020/04/09/technology/phone-calls-voice-virus.html; *Return of the Phone Call: Why Talking Beats Texting When You're in Isolation*, GUARDIAN (Mar. 17, 2020, 11:05 AM EDT), https://www.theguardian.com/lifeandstyle/2020/mar/17/return-of-the-phone-call-why-talking-beats-texting-when-youre-in-isolation.

320 Cecilia Kang, *The Humble Phone Call Has Made a Comeback*, N.Y. TIMES (Apr. 9, 2020), https://www.nytimes.com/2020/04/09/technology/phone-calls-voice-virus.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

period, internet traffic rose to twenty to twenty-five percent more than typical for the time.[321]

Increased use of phones, home internet connections, mobile devices, and Voice Over IP programs means an increase in risk exposure for consumers in regards to the privacy risks associated with these technologies. For example, the privacy risks associated with phone calls include potential for wiretapping as well as upstream surveillance from telecom providers as well as governments, who have many avenues of access to phone data.

The pandemic has also caused a shift in interpersonal privacy, the privacy that exists within social relationships. Social distancing has meant that more socialization has shifted to the online space, including gatherings of friends and family. Additionally, remote technologies have been used for dating and romantic relationships. In a time when many people have been encouraged to stay at home, and to maintain physical distance from others when outside the home, many have turned to online chat, SMS, voice, and video chat to engage in romantic activities.[322] The simple fact that more people are using these technologies for these purposes creates greater risk for abuse—including legally unprotected forms of sexual harassment,[323] stalking, nonconsensual pornography,[324] sexual deep fakes,[325] and more. It is also possible that individuals less versed in the dangers of online platforms in romantic contexts may now be using those platforms, leading to greater potential for harm.

---

321 Cecilia Kang, *The Humble Phone Call Has Made a Comeback*, N.Y. TIMES (Apr. 9, 2020), https://www.nytimes.com/2020/04/09/technology/phone-calls-voice-virus.html.

322 Olivia Carville & Nate Lanxon, *How to Date Online in the Age of Covid-19*, BLOOMBERG (Mar. 20, 2020), https://www.bloomberg.com/news/articles/2020-03-20/online-dating-in-a-pandemic-coronavirus-keeps-singles-apart; Vijai Nathan, *Date Lab: Our First Virtual Date*, WASH. POST (May 7, 2020, 6:00 AM EDT), https://www.washingtonpost.com/lifestyle/magazine/date-lab-our-first-virtual-date/2020/05/05/95f1aaca-7e5c-11ea-a3ee-13e1ae0a3571_story.html; Frances Perraudin & Sarah Marsh *Coronavirus Is Icebreaker for Online Daters—But Meeting Has to Wait*, GUARDIAN (Mar. 20, 2020, 1:40 PM EDT), https://www.theguardian.com/world/2020/mar/20/coronavirus-icebreaker-online-daters-meeting-wait; Melissa Schorr, *Blind Date: 'She Looked Like She Had Gotten Dressed up for Our Virtual Date,'* BOS. GLOBE (May 8, 2020, 8:18 AM), https://www.bostonglobe.com/2020/05/08/magazine/blind-date-she-looked-like-she-had-gotten-dressed-up-our-virtual-date

323 Mary Anne Franks, *Sexual Harassment 2.0,,* 71 MD. L. REV. 655 (2012).

324 Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014); Waldman, A. (2019); Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 L. & SOC. INQUIRY 987 (2019).

325 Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019); Mary Anne Franks & Ari Ezra Waldman, *Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions*,, 78 MD. L. REV. 892 (2019).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

Danielle Citron has theorized a right to sexual privacy, the privacy concerning not only sexual information and sexual activities, but also the privacy necessary to create room for human intimacy and intimate relationships.[326] It is important to understand sexual privacy in light of remote technologies, particularly in the midst of a pandemic that discourages in-person contact. Many of these technologies lack legal protections for privacy aside from the minimal U.S. sector-specific privacy protections. As Citron argues, current privacy laws do not adequately protect sexual-privacy interests. Citron calls for legal reform to protect sexual privacy, including potentially the creation of new legislation dedicated specifically to sexual-privacy rights.[327] The need for sexual-privacy protections is even more clear, as the pandemic has accelerated the adoption of new technologies in romantic contexts.

2. In-Person Consumer Surveillance

Corporations have also begun surveilling their consumers in physical spaces, in an effort to limit virus transmission. For example, some movie theaters have proposed privacy-invasive measures, including temperature scans and symptom questionnaires at the door.[328] In early May 2020, Disneyland Shanghai announced that it would reopen with enforced social distancing,[329] and Disney CEO Bob Iger has said the company has considered implementing temperature checks at the door.[330] It is possible companies could use technologies, including drone surveillance cameras, facial recognition, Bluetooth beacons, and more to enforce measures such as social distancing, mask wearing, and contact tracing.

Thus, individuals may find themselves the subjects of both government surveillance and corporate surveillance. While individuals have some recourse against government intrusions on fundamental rights, it is not so much the case with corporate surveillance. Thus, attention must be paid to corporations' use of consumer surveillance as response to the COVID-19 epidemic, as it is likely these surveillance measures will not immediately disappear once the pandemic

---

326 Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019).

327 Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019).

328 Gene Maddaus, *Texas Movie Theaters Reopen With Health, Temperature Checks*, VARIETY (May 1, 2020 2:00 PM PT), https://variety.com/2020/biz/news/texas-movie-theaters-reopen-coronavirus-1234595569.

329 Sarah Whitten, *Shanghai Disneyland Will Offer Disney a Blueprint for How to Reopen Its Other Theme Parks*, CNBC (May 6, 2020, 3:38 PM EDT), https://www.cnbc.com/2020/05/06/shanghai-disneyland-will-offer-a-blueprint-for-reopening-other-parks.html.

330 Jill Goldsmith, *Disneyland Could Start Temperature Checks When Parks Reopen, Bob Iger Says*, DEADLINE (Apr. 7, 2020, 4:06 PM), https://deadline.com/2020/04/disneyland-temperature-checks-coronavirus-reopen-plans-1202903111.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

has ended.

3. Digital Inequities

Children and young people may have unique experiences with privacy and technology in this public-health crisis. As schools have moved online and other activities have shut down, minor students have likely been using computers and mobile devices in an unsupervised capacity at higher rates than before. Children and young adults have been creative in their use of Zoom outside of educational uses—using Zoom for dating, parties, and other social engagements.[331] Children could be losing the safety that comes with having adult supervision by parents or teachers in some of their use of these technologies.[332] This raises greater potential for abuse, including privacy harms like harassment, cyberstalking, cyberbullying,[333] child targeting, nonconsensual pornography,[334] and other privacy violations, including sexual-privacy violations.[335]

Privacy harms related to communication via online or remote platforms are often worse for women and girls,[336] LGBTQ people,[337] people of minority status (based on race, religion, or other), disabled people, and other individuals who come from marginalized groups.[338] Algorithmic harms are often worse for many marginalized groups, as the effects of AI bias reflect the systemic biases in society. The increased use of technology, including privacy-invasive technology and AI-based systems, will likely have an unequal impact on privacy for different groups.

The lack of free, accessible remote communication technologies has not only disparately harmed the poor and people in rural communities, but it also

---

331 Taylor Lorenz et al., *We Live in Zoom Now*, N.Y. TIMES (Mar. 17, 2020), https://www.nytimes.com/2020/03/17/style/zoom-parties-coronavirus-memes.html.

332 Press Release, Cox Commc'ns, New Research Reveals Risky Internet Behavior Among Teens, but There Are Encouraging Signs of Improvement with Increased Involvement of Parents and Guardians COX COMMC'NS (May 10, 2007), http://www.cox.com/wcm/en/aboutus/datasheet/takecharge/archives/2007-risky-behavior.pdf.

333 Ari Ezra Waldman, *Triggering* Tinker*: Student Speech in the Age of Cyberharassment*, 71 U. MIAMI L. REV. 427 (2017).

334 Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014); Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 L. & SOC. INQUIRY 987 (2019).

335 Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.LawJ. 1870 (2019).

336 Anita L. Allen, *Gender and Privacy in Cyberspace*, 52 STAN. L. REV. 1175 (2000); ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988)

337 Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 L. & SOC. INQUIRY 987 (2019).

338 Scott Skinner-Thompson, *Privacy's Double Standards*, 93 WASH. L. REV. 2051 (2018).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

disproportionally harms incarcerated people and their loved ones. Incarcerated people already have few of the communication abilities people in the free world enjoy. As prisons have locked down visits, some facilities have also limited the ability for incarcerated people to access phones and computers (or in some cases, any shared spaces).[339] As remote videoconferencing technology explodes in usage elsewhere, the same cannot be said for jails and prisons. Incarcerated people already have few expectations of privacy, but here, better videoconferencing technologies could help restore human dignity to incarcerated people and their loved ones in the free world.

4. Legal and Regulatory Interventions to Protect Consumer Privacy

The law offers legal protections for communications privacy, including the Electronic Communications Privacy Act. The increased use of landlines and mobile telephone calls highlights the need for privacy protections over telephone communications, in addition to the protections needed for online communications.

However, the use of remote technologies highlights problems related to technology platforms, including those used for communication in a time of social distancing. One area of interest is intermediary liability, or the immunity protections certain internet platforms receive regarding some areas of liability. The increased use of remote working technologies that include photo, audio, or video also create greater content moderation, speech regulation, and online harassment concerns for tech platforms. In particular, the increasing importance of technology platforms in this public health crisis raise issues of platform governance, including issues of online harassment, speech, and liability (or immunity from liability), aiding the greater trend of tech platforms becoming what Kate Klonick has named "the new governors of speech."[340]

In the United States, many internet intermediaries are protected by Section 230, a law that provides immunity for certain platforms against some types of claims based on user-generated content on the platform.[341] Section 230 has been the subject of much debate among scholars, policymakers, and courts. Some argue that Section 230 is "the law that created the Internet,"[342] while others argue

---

[339] Joseph Shapiro, As COVID-19 Spreads imn Prisons, Lockdowns Spark Fear Of More Solitary Confinement, NPR (June 15, 2020 4:53 PM ET), https://www.npr.org/2020/06/15/877457603/as-covid-spreads-in-u-s-prisons-lockdowns-spark-fear-of-more-solitary-confinemen.

[340] Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018).

[341] 47 U.S.C. § 230 (2018).

[342] JEFF KOSSOFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

that the law allows for critical harms to privacy and civil liberties.[343] Congress amended Section 230 in 2018 with the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA),[344] leaving an opening for further erosion of Section 230 protection for platforms. While it remains to be seen how Section 230 protections will fare in the future, the myriad problems with technology platform power have become a pain point for many policymakers, particularly as momentum has built against the technology industry (referred to some as the "techlash[345]").

To regulate technology platforms, a privacy-forward approach must balance two competing privacy interests: the interests of individuals to protect their data from others; and the interests of individuals in being able to access a space that allows them the privacy to develop their own identities and pursue their intellectual and social interests.

III. RECOMMENDATIONS

A. Changing Privacy Norms

Our expectations of privacy (reasonable or not) are changing. The overall rise of the digital economy is certainly part of this change, but the integral roles of technology in this pandemic have also served to accelerate change in privacy norms. While it may be tempting to say that some of these changes will be limited to the time of pandemic, it is likely that changes in norms will have longer effects over time.

1. Blurring the Line Between Cyber and Physical Space

The pandemic pushed life indoors and online. As work, school, and social life all moved online, society has seen a further erosion in the division between the digital and the physical. Some of the privacy losses suffered in this pandemic have related to the loss of physical spaces. Students have lost the educational privacy afforded to them by the physical space of schools and universities. Employees have lost the privacy of their home, as remote employee surveillance

---

[343] See, e.g., Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 Fordham L. Rev. 401 (2017); Carrie Goldberg, NOBODY'S VICTIM: FIGHTING PSYCHOS, STALKERS, PERVS AND TROLLS (2019).

[344] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. Law. No. 115-164, 132 Stat. 1253. SESTA

[345] Rana Foroohar, *Year in a Word: Techlash*, FIN. TIMES (Dec. 16, 2018), https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e; Eve Smith, *The Techlash Against Amazon, Facebook and Google—And What They Can Do*, ECONOMIST (Jan. 20, 2018), https://www.economist.com/briefing/2018/01/20/the-techlash-against-amazon-facebook-and-google-and-what-they-can-do.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

has blurred the boundaries of space. The pandemic has also caused a crisis in interpersonal privacy, the privacy that exists within social relationships, as more relationships either play out in a remote, connected fashion, or are disrupted by the growing use of remote technologies in the home.

As society becomes increasingly digitized, with many essential functions of society taking place in the digital realm or through digital intermediaries, the distinction between digital and physical becomes increasingly meaningless. We are living through contextual shifts in how society understands the borders and limits of physical and digital spaces. Privacy law should attempt to protect cyber space as much as it protects physical space and digital privacy as much as it does physical privacy. This shift in norms has been slowly developing over time, and the pandemic's focus on remote socialization may have highlighted or quickened this change.

2. Privacy Is Essential for Public Health

Both public and private actors have used the public health emergency as a rationale for deployment of privacy-invasive technologies and technologically-influenced programs. Individuals have been asked to accept more and more privacy-violating technologies, in a number of spaces. At the same time, both physical and digital privacy have been threatened, all for the sake of pandemic response. However, there will always be another emergency. This is particularly apparent, as many of the technologies used in pandemic response are not entirely new technologies. What has changed is the shift in scale and the shift in justification for violations of privacy.

Society must protect the health of its people. We must remain vigilant about privacy incursions, because shifts in privacy norms now will lead to lasting repercussions even after the emergency has ended. We must also design these systems with purpose limitation for collection, use, and transfer of data, so that a system that collects data for public health will not later be used to infringe upon individual rights. Furthermore, for every technology and technologically-influenced response to this pandemic, there has always been a maximally secure and privacy-protecting version. Both state and private actors should consult with technologists and advocates in creating and implementing programs for public health response. Laws must be nimble enough to allow for flexibility, but with exceptions narrowly tailored to prevent privacy overreach due to purpose dilution.

Not only can privacy and public health co-exist, but privacy is essential for public health. As seen with the failure in digital contact app adoption, individuals will not willingly give their data to governments or companies if they cannot

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

trust that their privacy rights will be respected. This is problematic because pandemics and public health crises of all sorts require new technological innovations and technologically influenced solutions. To protect public health, we must protect privacy.

B. Law and Policy Recommendations

At time of writing, Congress is evaluating two competing bills dedicated to privacy and COVID-19.[346] Both bills address privacy protections for the data collection and tracking measures used in public health response. There does not appear to be enough political momentum to bring either bill to fruition, in an election year.[347] However, there is still time to use lessons from this pandemic to solve privacy issues for the future.

1. Sectoral Privacy Protection Is Not Enough

The pandemic's privacy impacts reach across areas of law, from consumer protection regulation to government surveillance law, and across different industries, from education to healthcare. It is difficult to grasp the full landscape of privacy in pandemic, due to the ever-expanding web of laws and regulations that touch upon privacy and technology. That difficulty, highlighted by the pressing urgency of the pandemic, is in itself one of the lessons to be gleaned from analyzing privacy and technology in this public health crisis. Regulating by data type and data setting does not work without overarching principles and cohesiveness between legal protections.

While limiting federal privacy regulation to specific laws for specific sectors may have been adequate for the early days of the internet and connected technologies, it is past time for Congress to pass a national privacy law that would provide cohesive, coherent rules based on core privacy values, that could then be translated to different sectors, industries, types of data, and types of data actors. The difficulty of protecting privacy in coronavirus testing is only one example of when the various sector-specific privacy laws fail to protect privacy or associate harms for individuals. The rising use of remote communication technologies in education is another such example, as even the strongest amalgamation of FERPA, COPPA, and FTC consumer protection law would not be enough to protect student or educational privacy. The sectoral privacy regime creates confusion, and the difficulty of compliance with conflicting

---

[346] COVID-19 Consumer Data Protection Act of 2020, S. 3663, 116th Cong. (2020); Public Health Emergency Privacy Act, S. 3759, 116th Cong. (2020).

[347] David Uberti, *Coronavirus Privacy Bills Hit Roadblocks in Congress,* WALL STREET JOURNAL (June 15, 2020), https://www.wsj.com/articles/coronavirus-privacy-bills-hit-roadblocks-in-congress-11592213400.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

requirements may hamper innovation and public health response. Differing state regulations compound that confusion, with some state laws becoming de facto regulations for the nation based on difficulty of compliance.[348]

A federal privacy law will be most useful in creating privacy values and standards across sectors, while still allowing for sectoral privacy laws to fill in the gaps. Technologies are constantly changing, as are uses of technologies, as we have seen with medical AI, telehealth communication technologies, and healthcare robots. Thus, it is more useful to create laws that allow for room for innovation and growth of industries, as opposed to laws that are overly restrictive, particularly in an omnibus regulation that seeks to govern many industries. For example, instead of regulating particular technologies, like healthcare robots, a federal privacy law could instead specifically regulate collection and use of data, as well as physical privacy violations caused by technologies with physical presence or embodiment.

2. Health, Biometric, and Genetic Privacy Laws Are Insufficient

The pandemic has highlighted the inadequacies of current laws in protecting sensitive health information, including biometric information, genetic information, and more. This is apparent if for no other reason than that the public health response to this global pandemic has generated the collection and processing of a vast quantity of data that could be considered health, biometric, or genetic data.

Any federal privacy law that seeks to govern all sectors must include protections for health information and other sensitive categories of information. A federal privacy law could serve to fill in some of the gaps of HIPAA, GINA, and other laws that govern health information. For example, a federal privacy law could protect patients when their data is collected by an actor that is not a HIPAA-covered entity or business associate (something that has occurred with some of the COVID-19 testing and contact tracing). It would also be wise to include some of the provisions from state health privacy laws, including biometric information privacy laws.

In lieu of a comprehensive federal privacy law, the U.S. needs stronger sectoral privacy laws that would govern health, biometric, and genetic privacy. Until a federal privacy law comes to pass, attention should be paid to updating existing laws to address the potential for violations of health privacy and genetic privacy. We should expand GINA to include greater protections against genetic

[348] For example, in managing compliance, organizations may set their standards to match the strictest state laws, making those state laws the de facto laws of the nation. Additionally, when creating new laws, policymakers often borrow from other states' laws.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

discrimination, including protection against disparate harms as Ifeoma Ajunwa has suggested, as well as protection against discrimination based on characteristics or health information that might not be categorized as genetic data. Additionally, we should expand GINA protections past the currently limited sectors of employment and health insurance discrimination to include fundamental rights such as education and housing. Furthermore, genetic privacy rights, including rights to donate data without fear of law enforcement access, should be expanded, either through a genetic privacy law or through provisions in a larger health or biometric privacy law.

Our current health privacy regime is insufficient to protect the privacy of what is perhaps the most sensitive data for any individual: biometric data, or data relating to or emanating from the body. Biometric data is particularly important to protect because such data is not only extremely identifiable but also intrinsically linked to our sense of selves. There's a fundamental difference between a data breach of credit card numbers versus a breach of face photos. We understand that difference intuitively, and individuals deserve stronger privacy protections for their sensitive biometric information, including health information and genetic information.

3. Privacy Law Must Address Digital Inequities

The pandemic has thrown into sharp relief the digital and economic inequities of modern life. No privacy law will ever fully protect the privacy of the people unless it takes into account inequities in privacy and technology. We should address discrimination as an information privacy harm, particularly related to algorithmic discrimination, which is based on information related to individuals. A federal privacy law should include protections for particularly vulnerable classes, as well as limitations on discriminatory uses of data (including disparate impact). These protections should be explicitly built into federal privacy law.

In lieu of a strong omnibus privacy law that includes protection against discrimination and disparate harm, other legal changes can help serve similar purpose. Laws that protect against harms that are often gendered or racialized can be helpful, including specific laws targeting harms like online harassment, cyberstalking, nonconsensual pornography, and swatting.[349] Additionally, laws that give more rights to data subjects, including algorithmic rights can help empower individuals who may suffer disproportionately from the harms of surveillance and algorithmic decision-making systems. One example is enforcing transparency and accountability for algorithms used in sentencing.

[349] For example, New York's non-consensual pornography law and a similar bill still stalled in Congress. https://www.nytimes.com/2019/02/28/nyregion/revenge-porn-law.html

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

4. Privacy Law Should Protect a Right to Educational Privacy

By shifting education to the digital space, and to the private home, the pandemic has exposed flaws in privacy protections for students and educators. Privacy law protects children as vulnerable classes under COPPA and FERPA. However, these protections are limited in types of data (student records for FERPA) and categories of data subjects and data controllers. We should reform education privacy laws to include protections ordinarily afforded to the physical educational space. Protection of educational privacy should transcend protection of children as a vulnerable class or school records as a sensitive form of data and should include instructors, researchers, and others engaged in the intellectual enterprise of education. Educational privacy protections should also be applicable to both public and private entities. This is but one failure in the current sectoral privacy regime, and one example of how the shifting privacy norms of cyber and physical space should change the way privacy law regulates.

5. Privacy-Forward Platform Regulation

The question of how to regulate technology platforms has risen to the forefront in recent years, and both policymakers and the general public have pressed for reform in a number of ways. The pandemic has exposed once again the integral role of technology companies and intermediaries in society, as technologies like remote videoconferencing apps and digital contact tracing apps have become important in COVID-19 response.

There are of course more problems with platform regulation than privacy. Internet intermediaries provide venues for speech to occur, and potential issues that must be raised for platform regulation include online speech access and expression, online harassment, election interference, disinformation, and more. Additionally, perhaps the greatest challenge in platform regulation today is not privacy or online speech but rather the power imbalance between increasingly powerful technology companies and people and governments. Some of this power imbalance is due to the vast quantity of data many of the large technology companies are able to collect, which has privacy implications but is not necessarily a privacy-exclusive issue.

Platform regulation must protect the privacy of individual consumers, as many have advocated for in calls to reform. However, the pandemic has also highlighted the gradual social shift of society in increasingly considering digital spaces as substitutions or supplements to physical spaces. Thus, it is crucial that intermediary regulation not overly restrict intermediaries such that they would no longer be able to provide the privacy of digital spaces that are necessary for

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

identity development, intellectual exploration, freedom of speech, and more. We must support privacy-forward platform regulation, separating the regulation of technology companies as economic actors and the regulation of intermediaries as venues for speech and connection.

6. Regulating Data Aggregators and Downstream Data Harms

The complex data cycles related to COVID-19 testing and contact tracing show the difficulty of regulating based on initial point of collection. Laws do not sufficiently protect against downstream harms, partly because it is difficult on a technical basis for anyone party involved in a data lifecycle to track all the different places data may go and different parties who may have access to said data.

It is time for regulation that addresses the compounded privacy harms of data aggregation. Currently, there are only a few state laws that address data brokers or data aggregators. A federal law that regulates data aggregators as an industry has the potential of protecting against myriad hams. Regulations that target data aggregators can include, but should not be limited to enforcing transparency about data sources that aggregators purchase and collect, as well as rights for individual data subjects to request access to data collected about them, as well as rights to correct and delete said data, and rights to opt out entirely from having their data be included as part of data sets used and sold by data aggregators. U.S. law includes some of these rights for some types of data aggregation, including laws allowing individuals to opt out of marketing mail, for example, as well as laws for algorithmic transparency in financial credit reporting.[350]

Many of the downstream data harms relate to the potential of data being misused as part of machine learning and algorithmic decision-making. U.S. law does not generally address rights related to algorithmic decision-making (with some exceptions), but the law should regulate situations where algorithmic decision-making can be used to make determinations that impact on fundamental rights.

CONCLUSION

This Article takes the particularities of the pandemic as a lens through which to gauge the progress of privacy protections across sectors, using the COVID-19 pandemic as a historical reference point. What is interesting about technology is not its novelty, but its salience. Similarly, what is interesting about studying

[350] Danielle Keats Citron and Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, Washington Law Review, Vol. 89 (2014).

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004

privacy in pandemic is not the novelty of the pandemic itself or the use of technology during these times, but rather what emerge as salient reflections on privacy, technology, and public health in society today.

The global COVID-19 pandemic has changed society in myriad ways, and it will take the long lens of history to understand the ramifications of this societal crisis. What is certain is that developments during this time, whether or not they relate to privacy and technology, will influence future directions for society. The data-driven programs developed as COVID-19 response, from viral testing to consumer communication technologies, have already transformed the way society interacts with technology and concepts of privacy. Our privacy norms are changing, and it is all but inevitable that the pandemic's effects will be long-lasting, with unforetold implications for our future society and its relationship with technology. As we progress toward that future, it is imperative that we create conceptions of privacy that are beneficial for society, as well as laws and regulations that protect both public health and civil liberties.

This Article provides a contemporary account of privacy, technology, and public health at this critical point in time. These situations will change as the pandemic progresses, comes to an end, and eventually, diminishes from the public sphere and public memory. As Teju Cole writes, in an essay on the difficulty of analyzing an in-progress pandemic, "History's first draft is almost always wrong—but we still have to try and write it."[351]

* * *

[351] Teju Cole, *We Can't Comprehend This Much Sorrow*, N.Y. TIMES (May 18, 2020), https://www.nytimes.com/interactive/2020/05/18/magazine/covid-quarantine-sorrow.html.

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=3690004