Hastings Science and Technology Law Journal

Volume 12
Number 1 *Winter 2020*

Article 5

Fall 2020

Katz and Covid-19 How a Pandemic Changed the Reasonable Expectation of Privacy

Wayne Unger

KATZ AND COVID-19: HOW A PANDEMIC CHANGED THE REASONABLE EXPECTATION OF PRIVACY

by WAYNE UNGER*

TABLE OF CONTENTS

* J.D., Arizona State university, Sandra Day O'Connor College of the Law, 2020.

ABSTRACT

COVID-19 spread to 189 countries and infected tens of millions of people in the matter of months. Organizations, including governments and employers, turned to health surveillance technologies to slow the spread and combat the disease. Protected health information and personal information are required for the proper and effective functioning of the health surveillance technologies. The collection, use, and dissemination of protected health and personal information raised data privacy and security concerns. But under the current data privacy and security regime—based on the reasonable expectation of privacy standard—protected health and personal information is not protected to the extent that it needs to be.

Unlike other scholarly work, this article presents deeper analysis into the technologies, the data that powers them, and the applicable legal standards. The objective is to provide a better understanding of (i) the data privacy and security risks, and (ii) whether the current data privacy and security regime in the United States provides sufficient protections for individuals.

This article explores two health surveillance technologies (contact tracing applications and health monitoring platforms), presents three categories of data (user-inputted, queried, and autogenerated data), and describes the data supply chains that power technology and organizations. I discuss the benefits and risks of collecting the protected health and personal information in response to the pandemic. I explore the current legal standards and jurisprudence, and I propose the Privacy Continuum to explain how the pandemic shifted the reasonable expectation of privacy. I present a case study to synthesize the foregoing, and I conclude by proposing a new legal standard—the right to control—and other reforms to effectuate true data privacy and security protections. Only then can we reclaim our right to privacy.

I. INTRODUCTION

On January 30, 2020, the World Health Organization ("WHO") declared the Coronavirus Disease 2019 ("COVID-19") outbreak a "public health emergency of international concern," and shortly thereafter, the WHO declared the outbreak a global pandemic.[1] On March 13, 2020, the President of the United States, Donald Trump, declared that the COVID-19 outbreak constituted a national emergency.[2]

As of November 2020, over 45 million people have been diagnosed with COVID-19 across 189 countries; over 1,200,000 of them have died.[3] In response to the pandemic, organizations, businesses, governments, and communities around the world mobilized to not only detect and contain the virus, but develop techniques (or methods) to treat those diagnosed with the disease.[4] Unlike past pandemics, the COVID-19 pandemic is occurring in a more connected and digitized world.[5] Accordingly, governments around the world have turned to technology to aid in their detection, containment, and treatment efforts relating to COVID-19.[6]

Israel tasked its intelligence agency to track COVID-19 patients by leveraging telecom data.[7] The United Kingdom deployed law enforcement drones to monitor public spaces and enforce social distancing practices.[8] Hong Kong and India installed geofencing technology to enforce quarantine zones.[9] South Korea, China, Taiwan, and many other countries, deployed smartphone applications for contact tracing.[10] Like other counties, United States politicians, businesses, and non-governmental organizations have called for or are

---

[1] *Timeline of WHO's Response to COVID-19*, WORLD HEALTH ORG. (Sept. 9, 2020), https://www.who.int/news-room/detail/29-06-2020-covidtimeline; *See International Health Regulations (IHR)*, CTR. FOR DISEASE CONTROL & PREVENTION, GLOBAL HEALTH PROTECTION & SECURITY (Aug. 19, 2019), https://www.cdc.gov/globalhealth/healthprotection/ghs/ihr/index.html (discussing the International Health Regulations [IHR] aim to keep the world informed about public health risks and events by requiring countries to have the ability to detect, assess, report, and respond to public health events).

[2] *Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak*, WHITEHOUSE.GOV (Mar. 13, 2020), https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/.

[3] *COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at John Hopkins University (JHU)*, JOHNS HOPKINS U. (Oct. 10, 2020, 1:23 PM), https://coronavirus.jhu.edu/map.html ("JHU Dashboard" provides case counts of confirmed and probable cases and the total number of cases and deaths are likely undercounts).

[4] *See generally* LEESA LIN & ZHIYUAN HOU, *Combat COVID-19 with Artificial Intelligence and Big Data*, J. OF TRAVEL MED. 1-4 (May 21, 2020), https://www.doi.org/10.1093/jtm/taaa080.

[5] Marcello Ienca & Effy Vayena, *On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic*, NATURE MED. 463 (Mar. 27, 2020), https://www.nature.com/articles/s41591-020-0832-5; *See Past Pandemics*, CTR. FOR DISEASE CONTROL & PREVENTION, INFLUENZA (FLU) (Aug. 10, 2020), https://www.cdc.gov/flu/pandemic-resources/basics/past-pandemics.html.

[6] *SEE* Liza Lin & Timothy W. Martin, *How Coronavirus Is Eroding Privacy*, WALL ST. J., (Apr. 15, 2020, 11:03 AM), https://www.wsj.com/articles/coronavirus-paves-way-for-new-age-of-digital-surveillance-11586963028.

[7] *Id.* at 1, 3.

[8] *Id.* at 1.

[9] *Id.* at 1.

[10] *Id.* (explaining that contact tracing is the process of identifying individuals who may have close contact with an infected person).

deploying various technologies to contain the spread of the virus.[11] While this article references efforts by other countries, it focuses specifically on the United States.

Protected Health Information ("PHI") is at the core of the technologies leveraged in the fight against COVID-19.[12] In aggregate, PHI is leveraged for data modeling, contact tracing, quarantine enforcement, symptom tracking, and the like.[13] However, privacy and security concerns regarding the collection, use, and dissemination of PHI are widespread..[14]

Individuals may believe that their PHI is protected under statutory, regulatory, or constitutional protections (e.g., the Heath Insurance Portability and Accountability Act ["HIPAA"] or the Fourth Amendment of the U.S. Constitution). Individuals may trust the data collectors' privacy, cybersecurity protocols, and technologies that are designed to protect Personal Information ("PI") or PHI.[15] But as individuals' willingness to share their PHI increases because of the pandemic, is their PHI and PI truly protected?[16] And if so, to what extent?

This article discusses the data privacy and security issues with respect to health surveillance technologies within the United States. This article is not an exhaustive analysis of the health surveillance technologies or the legality or constitutionality of the technologies. However, unlike other scholarly work, this article is a deeper analysis into

---

[11] *See generally* Adam Cancryn, *Kushner's Team Seeks National Coronavirus Surveillance System*, POLITICO, (Apr. 8, 2020, 12:19 AM), https://www.politico.com/news/2020/04/07/kushner-coronavirus-surveillance-174165 (describing the containment and surveillance efforts by the federal government and how it will use various technologies to combat COVID-19; I use the term "organizations" interchangeably with "companies" and "businesses" throughout this article. At times, I use the term "organizations" to include governments).

[12] *See* 45 C.F.R. § 160.103 (PHI includes information that (i) identifies, or can reasonably be used to identify, an individual; (ii) is created or received by a covered entity [e.g., health plan, health care provider, employer, or health care clearinghouse]; (iii) relates to an individual's physical or mental health, health care provision, or payment for provision of health care; and (iv) is transmitted by or maintained in electronic or any other format).

[13] *See generally* Carmel Shachar, *Protecting Privacy in Digital Contact Tracing for COVID-19: Avoiding a Regulatory Patchwork*, HEALTH AFFAIRS, (May 19, 2020), https://www.healthaffairs.org/do/10.1377/hblog20200515.190582/full/; *See also* Marcello Ienca & Effy Vayena *supra* note 5.

[14] *See* Cancryn *supra* note 11; AARON R. BROUGH & KELLY D. MARTIN, *Consumer Privacy During (and After) the COVID-19 Pandemic*, J. OF PUB. POL'Y & MKTG. (May 28, 2020), https://doi.org/10.1177/0743915620929999; Stephen P. Mulligan et al., DATA PROTECTION LAW: AN OVERVIEW, CONG. RES. SERV., (2019) (Data privacy relates to the control, use, and dissemination of personal information and PHI. Data security relates to (i) the protection of personal information and/or PHI from unauthorized access or use, and (ii) the response to the unauthorized access or use of the personal information or PHI); *See also* Chris D. Linebaugh, FACEBOOK'S $5 BILLION PRIVACY SETTLEMENT WITH THE FEDERAL TRADE COMMISSION, CONG. RES. SERV., (2019) (Data privacy and security concerns vary by person—not everyone has the same level of concern—and some may have no privacy expectations).

[15] *See* Art. 4 Global Data Protection Regulation ("GDPR") Definitions, (EU) (Data collectors are organizations that collect or store PI and PHI. For this article, data collectors include data processors [organizations that conduct a series of actions or operations using the data] and data controllers [organizations that determine the purposes and means of the data processing]); *See also Definition of Processes*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/processes. (last visited Oct. 10, 2020) (For this article, an example of PHI is a positive diagnosis of COVID-19, and two examples of personal information ("PI") are an individual's name and address).

[16] Anindya Ghose, et al., *Trading Privacy for the Greater Social Good: How Did America React During COVID-19*? SSRN (Aug. 15, 2020) (Working Paper, N.Y.U. STERN SCH. OF BUS.) http://dx.doi.org/10.2139/ssrn.3624069.

the health surveillance technologies and the applicable legal standards; the objective is to provide a better understanding of (i) the data privacy and security risks, and (ii) whether the current data privacy and security regime in the United States provides sufficient protections for individuals.

Part I discusses the health surveillance technologies. Part II explores various legal standards and jurisprudence with respect to data privacy and security and how privacy expectations have shifted and continue to do so since the pandemic began. Part II proposes a framework to visualize the legal standards and show the shift in privacy expectations. Part III presents a case study to show the legal standards as applied to deployed health surveillance technologies. Part IV argues that the current data privacy and security regime is ineffective and unworkable, and it proposes reforms to the data privacy and security regime to effectuate real consumer protections.

II. THE COVID-19 SURVEILLANCE TECHNOLOGIES

The COVID-19 disease spread to 188 countries and infected 28.5 million people in less than six months.[17] With the infectiousness of COVID-19, governments and organizations have turned to health surveillance technologies to help track and contain the spread.[18] At the core of these technologies is PI and PHI. And this data has quickly become more relevant and valuable during the pandemic for policy planning, workforce planning, diagnostics, stay-at-home order enforcement, and more.[19] The collection, use, and dissemination of this data raises data privacy and security concerns.

This Part I describes various health surveillance technologies, including how these technologies incorporate data privacy and security. Section A details two technologies: (i) contact tracing applications, and (ii) health monitoring platforms. Section B considers the data and data supply chains that underlay these technologies, including user-inputted data, queried data, and autogenerated data.[20] Lastly, Section C discusses the data privacy and security benefits and risks.

A. An Overview of Two Technologies in the COVID-19 Pandemic

Many technologies have been developed and deployed in response to the COVID-19 pandemic. But at least two technologies are concerning to privacy advocates and scholars: contact tracing applications and health monitoring platforms. This Section A provides an overview of these technologies, including some of the benefits and risks with respect to the data collection, use, and dissemination.

---

[17] *See* JMU DASHBOARD, *supra* note 3.

[18] Theodore Claypoole, *COVID-19 and Data Privacy: Health vs. Privacy*, A.B.A.(Mar. 26, 2020), https://www.americanbar.org/groups/business_law/publications/blt/2020/04/health-vs-privacy/.

[19] Cynthia Dwork, et al., *On Privacy in the Age of COVID-19*, J. OF PRIVACY & CONFIDENTIALITY (June 25, 2020), https://doi.org/10.29012/jpc.749.

[20] A data supply chain is the end-to-end flow of data across systems and technologies, including data suppliers and end-users. User-inputted data is data that is provided by the user (e.g., email address when creating a new account). Queried data is data obtained by the data processor by third-party data suppliers. Autogenerated data is data that is automatically captured or recorded; *See infra* Figure 1.

First, contact tracing applications are smartphone-based mobile applications that supplement or replace conventional contact tracing.[21] Conventional contact tracing involves manual interviews of infected individuals, conducted by public health authorities, that aim to collect information regarding who the infected individual physically contacted since becoming infected.[22] Because manual interviews of infected individuals are very difficult to scale during a global pandemic and alternative options exist today, governments and other organizations have turned to smartphone contact tracing applications that utilize geolocation data, either by the phone's Bluetooth, WiFi, or GPS.[23]

Organizations quickly developed and released contact tracing applications. Apple and Google partnered to develop the "Exposure Notification System," ("ENS") a privacy-preserving technology that uses Bluetooth, to help public health officials develop and launch their own contact tracing applications.[24] The ENS allows for iOS and Android devices to exchange beacons (similar to exchanging business cards) with other devices that have the ENS-based application installed.[25] For instance, if Jane Doe comes into contact with an infected individual (i.e., an individual who tested positive for COVID-19), then Jane Doe is notified via the ENS-based application by public health authorities.[26]

But Apple and Google are not the only organizations developing contact tracing technologies. In less than a month after the pandemic declaration, the Peruvian government launched a mobile application that uses GPS data for contact tracing.[27] Two months after the declaration, the South Korean government launched two applications, one of which was created by private developers.[28] Singapore, India, Israel, Hong Kong, Italy, and others also launched contact tracing applications since the pandemic began.[29]

In the United States, several contact tracing applications appeared on Google's Play and Apple's App Stores, some of which were not tied to a public health agency or

---

[21] Nadeem Ahmed, et al., *A Survey of COVID-19 Contact Tracing Apps*, CORNELL U., ARXIV.ORG (July 28, 2020), https://arxiv.org/abs/2006.10306.

[22] Ahmed, *supra* note 21, at 27 (explaining that contact tracing plays an important role in the control of infectious diseases, and how its value is widely accepted in public health globally); *See* Don Klinkenberg, et al., *The Effectiveness of Contact Tracing in Emerging Epidemics*, PLOS ONE (Dec. 20, 2006), https://doi.org/10.1371/journal.pone.0000012; *Contact Tracing*, WORLD HEALTH ORG. (May 9, 2017), https://www.who.int/news-room/q-a-detail/contact-tracing.

[23] Tony Romm, et al., *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, WASH. POST (March 17, 2020, 6:15 PM), https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/.

[24] Ryan Chiavetta, *Google, Apple Outline Privacy Considerations for Exposure Notification System*, INT'L ASS'N OF PRIVACY PROF'LS (June 26, 2020), https://iapp.org/news/a/google-apple-outline-privacy-considerations-within-exposure-notification-system/.

[25] *Id.*

[26] *Id.*

[27] Catherine Escobedo, *Geolocation and Other Personal Data Used in the Fight Against COVID-19*, INT'L ASS'N OF PRIVACY PROF'LS (last visited Oct 8, 2020), https://iapp.org/news/a/geolocation-and-other-personal-data-used-in-the-fight-against-covid-19/.

[28] Samantha Tsang, *Here Are the Contact Tracing Apps Being Deployed Around the World*, INT'L ASS'N OF PRIVACY PROF'LS (Apr. 28, 2020), https://iapp.org/news/a/here-are-the-contact-tracing-apps-being-employed-around-the-world/.

[29] *Id.*

authority.[30] Attorneys General from nearly forty states, as well as other policymakers and regulators, recognized that while contact tracing applications aid in combating the spread of COVID-19, many private companies may exploit the pandemic to collect PI or PHI.[31] New York's Attorney General, Letitia James, said, "some companies may seek to take advantage of consumers and use [PI] to advertise, mine [the] data, and unethically profit off this pandemic," and many likely do not know who or what is behind the efforts.[32] But regardless of whether the effort is a public-private partnership or wholly private endeavor, these efforts have received criticism from the general public and privacy experts regarding the data privacy and security capabilities.[33] The criticism is warranted because these applications collect, use, and disseminate PI and PHI.

Second, health monitoring platforms are software solutions that enable organizations to collect, store, and monitor PHI.[34] While the term "health monitoring platforms" is broad, for this article, I consider only the platforms that can be leveraged in response to the pandemic and are consumer-facing.

Health monitoring platforms have various purposes, features, and capabilities. For example, Safe Health Systems, Inc. ("SAFE") sells a platform that provides diagnostics, health record management, provider services, and the like.[35] FamHis, Inc. sells a white label platform (more on white label platforms below), FamGenix, that focuses on collecting family health history information.[36] Advancia Technologies and RingMD jointly sell a COVID-19 risk mitigation platform that allows for patient risk assessments, triage, and contact tracing.[37] And in April 2020, Pager, Inc. ("Pager") released its white label COVID-19 solution that offers health providers triage, risk assessment, and telemedicine capabilities.[38]

Other software platforms may not be designed for healthcare applications, yet they incorporate features and capabilities that are valuable to the pandemic's response. For example, human capital management ("HCM") platforms are designed for human resources departments to manage new employee onboarding, payroll, compensation, and the like. But many HCM platforms, like the Dayforce product from Ceridian HCM, Inc., have features that map the location of employees.[39] Employee mapping help employers

---

[30] Allison Grande, *Apple, Google Urged to Ax COVID-19 Apps With No Gov't Ties*, LAW360 (June 16, 2020, 10:25 PM), https://www.law360.com/articles/1283641/apple-google-urged-to-ax-covid-19-apps-with-no-gov-t-ties.

[31] *See generally id.*

[32] Grande, *Supra* note 30.

[33] *See* Chiavetta, *supra* note 24.

[34] Rachel Ranosa, *COVID-19: 6 Apps to Monitor Employee Health*, HUM. RES. DIR. (Apr. 22, 2020), https://www.hcamag.com/us/specialization/hr-technology/covid-19-6-apps-to-monitor-employee-health/220371.

[35] SAFE HEALTH SYSTEMS, INC., https://safehealth.me (last visited Oct 8, 2020).

[36] FAMHIS, INC., https://famgenix.com/white-label/ (last visited Oct 8, 2020).

[37] *COVID-19 Needs & Resources Matching*, NAT'L GOVERNORS ASS'N, (last visited Oct 8, 2020), https://www.nga.org/coronavirus-resources/.

[38] PRESS RELEASE, *Pager's New COVID-19 Solution Aims to Help Flatten the Curve*, PAGER INC. (Apr. 2, 2020), https://www.businesswire.com/news/home/20200402005294/en/Pager's-New-COVID-19-Solution-Aims-Flatten-Curve.

[39] *See* Ranosa, *supra* note 34.

understand whether their employees are at home or at the office, the chances of exposure to the virus, and the risk of infection.[40]

Health monitoring platforms can be white label platforms—fully developed and supported software solutions made by one company but sold to and used by another company.[41] For example, a multinational corporation may embed the Pager platform into its internal mobile application, and it could require all of its employees to complete an initial risk assessment before its employees can return to the office.[42] A high risk employee may be prohibited from returning to the office.[43] White label platforms significantly reduce the development requirements, which in turn, allow organizations to deploy a solution more quickly.[44]

Like contact tracing applications, the health monitoring platforms collect PI and PHI. In the employer-employee example, the employee submits multiple data elements, such as symptom status, health history, or travel history. The data is collected and stored by the platform provider (e.g., Pager) or the employer.[45] This raises data privacy and security concerns.[46] Using a platform, or manually collecting this data, employers can collect significant amounts of PHI from its employees, which can be vulnerable to data privacy or security risks if improperly collected, accessed, handled, used, or processed.[47]

The technologies deployed to combat the spread of COVID-19 are becoming the next treasure trove of PI and PHI. These are two examples; other technologies are omitted from this overview, but nonetheless, others are collecting the PI and PHI. With the collection, use, and dissemination of PI and PHI via these technologies and the organizations behind them, the concerns about data privacy and security are warranted. To better understand why data privacy and security concerns are warranted, I turn to an overview of the data and data supply chains.

B. An Overview of the Data and the Data Supply Chains of COVID-19 Technologies

Data is at the core of the technologies deployed to combat COVID-19. A technology solution is only as valuable as the data the solution collects, stores, and uses to deliver its capabilities and meaningful insights to organizational leaders.[48] This Section B presents an

---

[40] *Id.*

[41] Drew Gainor, *Why a White Label Solution Is Easier Than Building Your Own*, FORBES (June 3, 2014, 9:00 AM), https://www.forbes.com/sites/theyec/2014/06/03/why-a-white-label-solution-is-easier-than-building-your-own/#14e8aa3bdd9e.

[42] *See generally* Gainor, *supra* note 41.

[43] *See generally id.*

[44] *See* Carla Tardi, *White Label Product*, INVESTOPEDIA (last updated July 7, 2020), https://www.investopedia.com/terms/w/white-label-product.asp.

[45] *See, e.g.*, NGA ADVANCIA AND RINGMD PRESENTATION, *supra* note 37 (the Advancia and RingMD platform is hosted by cloud providers [e.g., Amazon Web Services] or on-premise [i.e., in the deploying company's data centers and servers]).

[46] *See generally*, Jedidiah Bracy, *OSHA Revises Guidance on Tracking COVID-19 in the Workplace*, INT'L ASS'N OF PRIVACY PROF'LS (June 1, 2020), https://iapp.org/news/a/osha-releases-guidance-on-tracking-covid-19-in-the-workplace/.

[47] *See generally id.*

[48] Other technologies (e.g., thermal imaging, biometrics, telemedicine, 3D printing, etc.) deployed to combat the pandemic leverage substantial amounts of PI and PHI; *See generally The Top 5 Practical Digital Health*

overview of data and data supply chains to illustrate the data ecosystem.[49] Without the understanding of the data ecosystem, one is limited in evaluating the data privacy and security risks.[50] And without the understanding of the risks, one cannot form effective protections for individuals against those risks.[51]

I start by distinguishing data into three categories—user-inputted, queried, and autogenerated. Next, I describe how the data categories play into a company's data supply chain. Last, I detail how companies use the data while leveraging other technologies, such as machine learning ("ML") and artificial intelligence ("AI").

There are three types of data: (1) user-inputted data, (2) queried data, and (3) autogenerated data (Figure 1). User-inputted data includes basic data elements that a user provides the software or application herself (e.g., name, email, phone). Queried data includes the data about an individual that is *sourced* from third parties. For example, to open a credit account at a bank, the bank will query data from a credit bureau (e.g., credit history and score) before decisioning the credit application. Autogenerated data is generated and collected about an individual through automation (e.g., behavioral analytics of a user and her interactions with a website). For Figure 1, I use the Five Building Blocks of Identity (Figure 1.1) ("Building Blocks") to describe how the three categories of data are used.[52]

Technologies in the Fight Against COVID-19: An Infographic, MEDICAL FUTURIST (May 7, 2020), https://medicalfuturist.com/the-top-5-practical-digital-health-technologies-in-the-fight-against-covid-19-an-infographic/.

[49] The term "data supply chain" includes the end-to-end processes, systems, and organizations used to collect, store, use, and disseminate data. This could include data providers, such as data brokers, and data storage providers, such as Amazon Web Services. This could also include data processors, such as ML / AI providers that process the data to derive analytics, insights, and the like.

[50] *See infra* Part I.C.

[51] *See infra* Part IV.

[52] Kaelyn Lowmaster, ET AL., *Digital Identity: The Foundation for Trusted Transactions in Financial Services*, CAPCO (Apr. 30, 2018), https://www.capco.com/Capco-Institute/Journal-47-Digitization/Digital-Indentity-The-foundation-for-trusted-transactions-in-financial-services.

Figure 1. Data Categories Chart

	Description	Source of Data	Used For	Example(s)
User-Inputted Data	Data that a user provides the data collector.	User	Creation Verification Authentication Authorization Federation	Name, Address, Phone Number, Zip Code
Queried Data	Data that a data collector sources.	Internal Systems or Third Parties	Verification Authentication Authorization Federation	Credit Report and Score
Autogenerated Data	Data that is created and collection via automation.	Internal Systems or Third Parties	Verification Authentication Authorization	Behavioral Analytics, User Interactions

Figure 1.1. Five Building Blocks of Identity[53]

Creation	Verification	Authentication	Authorization	Federation
The process of demarcating attribute(s) of an individual or entity such that the attribute(s) can be used in future	The process of confirming at least one attribute of an individual or entity, either through self-attestation or third-party confirmation.	The process of determining that one is transacting with the same individual or entity iteratively over time.	The process of determining the rights or privileges an individual or entity should be granted.	The process of conveying an individual's or entity's verification, authentication, or authorization information to another party.

[53] Lowmaster, *supra* note 52, at 146.

transactions to prove existence and uniqueness.				
Who are you?	**How do we prove who you are?**	**How do we know it is still you?**	**What do you get once we know it is you?**	**How can we tell other people it is you?**

Individuals often believe that the data collected by companies is either (i) the data that a user inputs into the software (e.g., name), or (ii) the data that the user generates via her interactions with the software *that the user can see* (e.g., total dollar amount of an eCommerce transaction).[54] But this is an elementary understanding of the data ecosystem because user-inputted data is only a part of picture—it neglects queried data and autogenerated data.[55]

While the majority of Americans acknowledge they are being tracked, 79% of adults state they have little to no understanding about what the government does with their data, and this is likely the same percentage with respect to the private sector.[56] For instance, when asked about what privacy means, one survey respondent stated, "My personal information is secure. No one knows my credit card numbers, address info, where I have been, my banking info, my health info, etc. People don't know anything about me I do not

[54] For this article, user-inputted data includes both the data that a user inputs into the software and the data that the user generates via her interactions with the software. The latter is distinguished from autogenerated data because autogenerated data is not necessarily produced as an outcome of a user's inputs or interactions with the software—this data the user *can see* for herself or himself. For instance, while an eCommerce transaction's total dollar amount is automatically calculated, the calculation is a *result of the user's input*, and autogenerated data could be the browsing analytics (e.g., how long a user remains on a page, the clickthrough rates, etc.) that the user *cannot see* herself.

[55] *See* Emily Stewart, *Lawmakers Seem Confused About What Facebook Does – and How to Fix It*, VOX (Apr. 10, 2018), https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations (detailing the lack of understanding by Congress and stating, "[p]lenty of people have a very limited notion of how exactly Facebook's business works, what happens to their data, and what they can do to increase their privacy."); *See, e.g.*, Brittany Martin, Note, *The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era*, 105 IOWA L. REV. 865, 870-72 (2020) (explaining that data brokers get data from publicly available records kept by governments, social media and blogs, and commercial sources (e.g., retailers). But Martin's article fails to consider queried and autogenerated data that most users are not aware is being tracked, stored, used, and disseminated).

[56] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* 10, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf (a total of 4,272 panelists responded to the survey out of the 5,869 sampled. The survey was conducted between June 3-17, 2020, with the response rate of 73%. The margin of sampling error for the 4,272 respondents is ±1.9%. For the survey's methodology, *See* AUXIER at 46-47. "Tracked" means the monitoring by companies and the government with some regularity); *See also* Brian Mastroianni, *Survey: More Americans Worried About Data Privacy Than Income*, CBS NEWS (Jan. 28, 2016), https://www.cbsnews.com/news/truste-survey-more-americans-concerned-about-data-privacy-than-losing-income/ (discussing a survey by TRUSTe/National Cyber Security Alliance regarding Americans and data privacy).

intend to share."[57] This response demonstrates an elementary understanding of what data is collected—if the concept of data privacy for 79% of Americans extends insofar as surface-level PI, such as credit card numbers, then it suggests that 79% of Americans are likely not aware of the totality of data at play.

User-inputted data is only a piece of the pie—an organization can query user-inputted data to obtain more PI than what the user provided. For instance, Company X may collect the name, address, and email address from the user, and it can query these data elements with a third-party provider, such as Neustar, Inc. ("Neustar").[58] Company X sends Neustar the data elements, Neustar's product matches the individual with its database, and then Neustar populates any missing data, such as the individual's telephone number, age, gender, income level, etc.[59] The data that Neustar provides Company X is the *queried* data.

Both Company X and its third-party data provider form Company X's data supply chain—Neustar being a data supplier to Company X. Company X maintains a more extensive data supply chain. Company X may want to track the behavioral data and analytics (autogenerated data) of its users who visit its website or use its mobile application. Company X could use Hotjar Ltd.'s ("Hotjar") product that provides Company X with user heatmaps, funnels, recordings, and more.[60] With Hotjar, Company X can track how users click-through, tap, and scroll through its website.[61] It can identify where its users are exiting the website using Hotjar's funnel feature.[62] And with Hotjar's Recording feature, Company X can watch recordings of users' interactions and behaviors on its website.[63] By embedding Hotjar into its platform, Company X *autogenerates* data—data that many individuals are likely not aware of given the 79% of Americans who hold a limited understanding of data collection.[64]

Now, Company X has two data suppliers—Neustar and Hotjar—each providing Company X with different sets of information that Company X can leverage for decisioning (Figure 2). But a user may not care about the traditional PI and behavioral analytics tracking. The user may be more concerned with her geolocation data because geolocation data is more sensitive than traditional PI; 82% of adults feel that the details of their physical location is somewhat or very sensitive.[65] Even the Supreme Court recognizes geolocation data is of great concern with respect to one's privacy.[66]

---

[57] Auxier, *supra* note 56, at 13.

[58] *See* NEUSTAR, INC., https://www.cdn.neustar/resources/product-literature/marketing/neustar-marketing-customer-identity-file-solution-sheet.pdf (last visited Oct. 9, 2020) (Neustar provides real-time data to organizations across four main product lines: marketing, risk, communications, and security solutions).

[59] *Id.*

[60] *See* HOTJAR LTD., https://www.hotjar.com (last visited Oct. 9, 2020).

[61] *See Heatmaps*, HOTJAR LTD., https://www.hotjar.com/tour/#heatmaps (last visited Oct. 9, 2020).

[62] *See Conversion Funnels*, HOTJAR LTD., (last visited July 22, 2020).

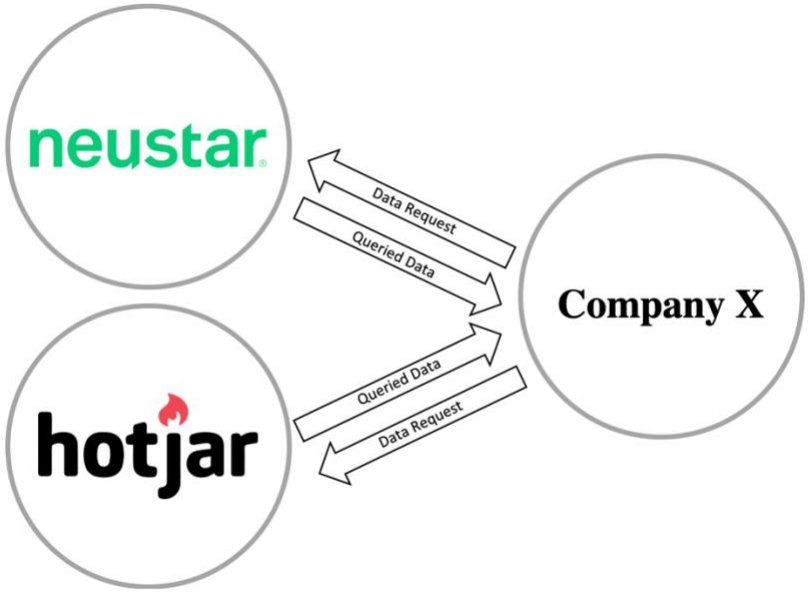
[63] *See Visitor Recordings*, HOTJAR LTD., https://www.hotjar.com/tour/#recordings (last visited Oct. 9, 2020).

[64] *See* Auxier, *supra* note 56.

[65] Mary Madden, *Americans Consider Certain Kinds of Data to Be More Sensitive than Others*, PEW RSCH. CTR. (Nov. 12, 2014), https://www.pewresearch.org/internet/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/.

[66] *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (recognizing that when the Government tracks the geolocation data of one's cell phone, the Government "achieves near perfect surveillance, as if [the Government] attached an ankle monitor to the phone's user."); Riley v. California, 573 U.S. 373, 393 (2014)

Figure 2. Company X's Data Supply Chain



Turning back to the Neustar example, Company X may automatically collect the IP address when the user visits its website. Company X can send the IP address to Neustar, and Neustar can return more than 40 data elements including the IP's continent, country, state, city, zip code, latitude and longitude.[67] Company X can identify the user's geolocation to the specific longitude and latitude using just the user's IP address.

A user's geolocation is autogenerated data and is critical to digital contact tracing.Mobile devices locate themselves using a variety of signals from satellites (GPS), cell towers, WiFi networks, Bluetooth signals, and proximity to other devices.[68] Carriers, the device's operating system, applications, data brokers, other third parties use the geolocation data from a mobile device.[69] Even if a user's PI is removed from the data set (e.g., if Company X separates a user's name from her geolocation data), geolocation data can be traced back to the specific user because geolocation data contains information regarding the user's "sensitive locations," such as the user's home and office locations.[70]

(recognizing that modern cell phones "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, wallet, or purse.").

[67] *See UltraGeoPoint Provides Insight into 99.99% of All Routable IP Addresses*, NEUSTAR, INC. 1 (May 12, 2020), https://www.cdn.neustar/resources/product-literature/security/neustar-ip-geopoint-solution-sheet.pdf.

[68] Stacey Gray, *The World of Geolocation Data*, FUTURE OF PRIVACY F. (May 22, 2020), https://fpf.org/2020/05/22/understanding-the-world-of-geolocation-data/.

[69] *Id.*

[70] *Id.*; *See* Sarah Underwood, *Can You Locate Your Location Data?*, COMMC'NS OF THE ACM (Sept. 2019), https://www.doi.org/10.1145/3344291 (detailing how users often lack the awareness that mobile applications collect location data, including applications such as Snapchat and Tinder).

It is possible for autogenerated data to be sourced from a third party. In other words, what is queried data for one organization may be autogenerated data for another organization. For example, even though the Secret Service does not collect geolocation data itself, it sources the data from third party suppliers—often avoiding the warrant requirement.[71]

This data (user-inputted, queried, and autogenerated data) can be combined with other technologies, such as ML and AI. Public health authorities, researchers, and experts are leveraging ML-based technologies to study COVID-19, test potential treatments, diagnose patients, analyze public impacts of the pandemic, and model the spread of COVID-19.[72]

For example, Chinese doctors used AI to leverage data from the first onset of COVID-19 to detect disease using chest CT scans.[73] Their efforts resulted in a deep learning model that accurately detects COVID-19 and differentiates it from other lung diseases.[74] The construction of any deep learning module with this objective requires big data sets of individuals' PI and PHI.[75]

For these technologies to function properly, the software requires the user's PI and PHI to develop and test the application. Moreover, ML and AI require massive data sets to train the software and its functionality.[76] Here, the software is only as valuable as the data the software collects, stores, and uses. It is not unforeseeable that this data could be applied to a variety of other applications, such as governmental health surveillance after the pandemic ends. Using the data in other applications than originally intended is one example of a data privacy and security risk—the topic that I turn to next.

C. A Discussion Regarding Data Privacy and Security Risks

The amount of data being collected, used, stored, and disseminated in response to COVID-19 brings serious risks. This Section C describes several benefits and risks associated with health surveillance technologies that collect substantial amounts of PI and PHI. First, this section explains how the aggregation of large data sets is benefitting the response to COVID-19. Then, it presents the possible abuses of the data during and after the pandemic. Second, I describe the risk and consequences of a data breach. And third, I detail how the risks apply to the individual, and it balances the risks against the public health benefits in response to the pandemic.

There is a trade off with the collection of PI and PHI in response to the pandemic—balancing an individual's right to data privacy against the public health need in combating COVID-19. With the clear public health interest, it is necessary to collect some level of PI and PHI to deploy the health technologies that will assist in slowing the spread, but the question becomes *what is the optimal combination of COVID-19 response tactics that*

---

[71] Amanda Yeo, *The Secret Service Bought Phone Location Data, Dodging the Need for a Warrant*, MASHABLE (Aug. 19, 2020), https://sea.mashable.com/tech/12013/the-secret-service-bought-phone-location-data-dodging-the-need-for-a-warrant.

[72] Brenda Leong & Dr. Sara Jordan, *Artificial Intelligence and the COVID-19 Pandemic*, FUTURE OF PRIVACY F. (May 7, 2020), https://fpf.org/2020/05/07/artificial-intelligence-and-the-covid-19-pandemic/.

[73] *Id.*

[74] *Id.*

[75] *See id.*

[76] ML and AI require large data sets to train the technologies' functionality. S*ee* LEONG, *supra* note 72 (quality of system dependent on quality of data).

allow for the suppression of the virus and disease but at a low human, civil, and economic cost?[77]

The goal of collecting the PI and PHI during and after the pandemic is to eradicate the virus and disease.[78] Stefan Pollinger, a researcher at Toulouse School of Economics in France, argues that the optimal combination of social distancing and case detection (e.g., contact tracing) allows for the suppression of COVID-19 at low additional human and economic costs (e.g., the costs associated with individuals' privacy) if the proper balance is struck between social distancing and case detection—where social distancing decreases the growth rate of COVID-19 by reducing the contact between individuals and case detection isolates infectious individuals from the susceptible population.[79] Social distancing is costly, and it becomes inefficient when the prevalence of COVID-19 is low.[80] When the prevalence is low, public health authorities can concentrate resources towards case detection, where the detection rate and efficiency of detection increase when the prevalence is low.[81] Taken together, these complementary responses to COVID-19, when optimally balanced, curtail the cost of suppression.[82]

In Pollinger's optimal suppression theory, PI and PHI add value to both sides of the equation; the data can be used to track social distancing, and the data can be used in case detection—key benefits to the aggregation and mining of large data sets. For example, for social distancing tracking, location data from Apple's navigation application, Maps, can be aggregated to track societal movement.[83] Further, OpenTable data can track restaurant bookings.[84]

However, as Pollinger and other scholars note, the risks of collecting the PI and PHI are also present.[85] While the purpose of collecting the PI and PHI may be for contact tracing and health monitoring, the data may be used after the pandemic ends for other purposes; this is known as *mission creep* or *function creep*.[86] Function creep is when data is collected

---

[77] *See generally* Stefan Pollinger, *COVID-19: Suppression Is Possible but at What Cost to Our Privacy?*, WORLD ECON. F. (July. 8, 2020), https://www.weforum.org/agenda/2020/07/suppressing-covid-19-with-a-combination-of-social-distancing-and-case-detection/ (theorizing the eradication of COVID-19 is possible through a combination of contact tracing, case detection, and social distancing—all of which could have a low civil, human, and economic cost).

[78] *See id.*

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] *See* Alex Harring & Nate Rattner, *Here Are Five Charts Illustrating U.S. Economic Trends Amid the Coronavirus Pandemic*, CNBC (July 19, 2020. 9:15 AM), https://www.cnbc.com/2020/07/19/five-charts-illustrating-us-economic-trends-amid-coronavirus.html (Compared to the baseline pre-pandemic average, the change in volume of navigation requests decreased by approximately 50% at the end of March into May 2020).

[84] *Id.* (OpenTable is a mobile application that allows users to make restaurant reservations. It reported a 100% decline in restaurant bookings via its mobile application at the end of March into May 2020).

[85] *See generally* Pollinger, *supra* note 77 (including privacy as an economic and health cost of the optimal suppression theory).

[86] *See* Dwork, *supra* note 19, at 1; *See also* Wendy Mariner, *Mission Creep: Public Health Surveillance and Medical Privacy*, 87 BOS. U. L. REV. 347 (2007) (discussing public health surveillance programs and mission creep in the health sphere); Evelina Manukyan & Joseph Guzzetta, *How Function Creep May Cripple App-Based Contact Tracing*, INT'L ASS'N OF PRIVACY PROF'LS (May 27, 2020), https://iapp.org/news/a/how-function-creep-may-cripple-app-based-contact-tracing/# (refers to mission creep as function creep).

for one purpose but is then used for other purposes, which often stray from the original intention.[87]

For example, PI collected for a contact tracing application, when used for other purposes and combined with other data sets from a company's data supply chain, can reveal social and political contacts.[88] This data could reveal an individual's daily routine, and with function creep, this data can be leveraged for marketing and advertising purposes or to compromise the individual's safety and security.

Several scholars and practitioners advocate for data minimization to prevent function creep.[89] However, there are two issues with data minimization, especially with respect to collecting PI and PHI in response to the pandemic: (i) organizations are not incentivized to practice data minimization, and (ii) even if an organization practices data minimization with respect to collecting PI and PHI *from the individual*, the organization is still able to pair the data collected to its queried or autogenerated data. Organizations are not incentivized to minimize their data collection because most organizations monetize the data—a crucial part of their business models.[90]

Several contact tracing applications state that they practice data minimization—going as far as claiming *no* PI is collected.[91] Researchers from the University of California, Irvine ("UC Irvine") proposed an application that "respects user privacy by not collecting location information or other personal data."[92] Their proposed application would use checkpoints in lieu of geolocation tracking—users would create new or join existing "checkpoints."[93] To check-in, users scan a QR code.[94] Users can voluntarily report a positive COVID-19 diagnosis, and any user can check their "risk level" by reviewing their exposures to possible transmission routes.[95]

Here, while the researchers at UC Irvine, in theory, created a contact tracing application that protects privacy via data minimization, the application is unrealistic because the application's design will not generate the user adoption necessary for the application to be effective. The user experience (e.g., the use of QR codes) requires affirmative actions by the user, and the application's core function relies on users taking these affirmative actions.[96] Each action required by the user creates friction in the user experience, and each friction point increases the probability that a user will not complete the end goal (creating

[87] Manukyan, *supra* note 86.
[88] Dwork, *supra* note 19, at 1.
[89] *See* Jennifer Baker, *Pandemic Incites Concerns About Data-Sharing Overreach*, INT'L ASS'N OF PRIVACY PROF'LS (Mar. 26, 2020), https://iapp.org/news/a/global-pandemic-incites-concerns-about-data-sharing-overreach/; Data minimization is when an organization or product only collects the data that the organization or product needs to collect and deletes any data that the organization may have collected but no longer needs.
[90] *See id.* (noting that Google may have altruistic reasons for collecting PI and PHI during the pandemic, but Google unequivocally leverages PI to generate revenue).
[91] *See, e.g.*, Tyler Yasaka et al., *Peer-to-Peer Contact Tracing: Development of a Privacy-Preserving Smartphone App*, 8 JMIR MHEALTH UHEALTH (July 4, 2020), https://mhealth.jmir.org/2020/4/e18936.
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*

and checking into checkpoints by scanning QR codes).[97] This is especially true today because frictionless or friction-minimal user experiences have become the norm.[98]

A frictionless or friction-minimal user experience will require some level of PI and PHI collection, sharing, and usage.[99] Because of this, several scholars and practitioners advocate for data anonymization.[100] But as previously explained, even if "anonymous" or non-identifiable data is collected, such data cannot be truly anonymous because the data can be linked to individuals through "reidentification."[101] The data collector can source PI and PHI to "fill in the gaps," and by doing so, it can link the data sets together to reconstruct the personal identity profile.[102]

While an organization may rely on its data suppliers, there are other methods that an organization may pursue to collect PI and PHI that do not require a third-party supplier. The PI and PHI that an organization collects can be combined with data scraped off the internet.[103] If Clearview AI, a startup that has collected over three billion photos of individuals by scraping the internet, can compile a massive database of PI via internet scraping, then any organization or malicious actor can do the same.[104] Between scraping the internet and sourcing queried data, organizations can take the pandemic-related PI and PHI and capitalize on it in other ways.

Considering the sources that an organization can leverage to gather data (collecting PI and PHI themselves, sourcing data from its supply chain, and scraping data), an organization can leverage other technologies, such as AI and ML, to use and mine the data—gathering insights, identifying monetization opportunities, exploiting psychology to influence individuals, etc. Dr. Dipayan Ghosn, the Pozen Fellow at the Shorenstein Center on Media, Politics and Public Policy at Harvard Kennedy School and former Policy Advisor in the Obama White House, notes, "the industry's goal is to enter our mind and move our psychology," and considering that AI and ML mature organically by learning

---

[97] *See* Victoria Young, *Strategic UX: The Art of Reducing Friction*, TELEPATHY (A SERVICENOW COMPANY), https://www.dtelepathy.com/blog/business/strategic-ux-the-art-of-reducing-friction ("friction is defined as interactions that inhibit people from intuitively and painlessly achieving their goals within the digital interface. Friction is a major problem because it leads to bouncing, reduces conversions, and frustrates would-be customers to the point of abandoning their tasks.").

[98] *Id.*

[99] Friction-minimal user interface design is defined as creating a user experience that minimizes the friction points, which in turn, decreases bouncing, increases conversion rates, etc.

[100] *See* Liane Colonna, *Privacy, Risk, Anonymization and Data Sharing in the Internet of Health Things*, J. OF TECH. L. & POL'Y (2020), https://www.doi.org/10.5195/tlp.2020.235/ (assessing data anonymization as a risk mitigation strategy to reduce privacy concerns in the "Internet of Health Things").

[101] *See id.*; *See also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

[102] *See supra* Part I.B.

[103] Internet scraping is the process of creating a bot (software code) to pull or download information or data from websites; *See, e.g.*, David Conrad, *"Scraping" of a Publicly-Accessible Website Database May Be Misappropriation of Trade Secrets*, JD SUPRA (July 14, 2020), https://www.jdsupra.com/legalnews/scraping-of-a-publicly-accessible-33549/ (explaining an Eleventh Circuit holding in a case that involved internet scraping).

[104] *See* Davey Alba, *A.C.L.U. Accuses Clearview AI of Privacy 'Nightmare Scenario'*, N.Y. TIMES (June 3, 2020), https://www.nytimes.com/2020/05/28/technology/clearview-ai-privacy-lawsuit.html; *See also* Ben Kochman, *Privacy and Cybersecurity Cases to Watch in 2nd Half of 2020*, LAW360 (July 24, 2020), https://www.law360.com/articles/1290397.

from data sets, the influencing of one's psychology is "an experimentally and empirically evolved animal (AI/ML) trained to identify opportunities for economic arbitrage."[105] Despite the altruistic statements by organizations that have sought or are seeking to collect the PI and PHI during the pandemic, as Ghosh argues, "there is no incentive for [organizations] to delete the [PI] they have already accumulated [because data] contribute[s] to the high margins experienced across the sector."[106]

With the constant data collection and usage, often leveraging AI and ML, data is created every second.[107] These massive databases of PI and PHI are subject to data breaches.[108] And the healthcare industry is slowest at identifying or detecting a data breach after one occurred, which amplifies the risk.[109] On average, the healthcare industry takes 236 days to identify a breach and then 93 days to contain the breach.[110]

Therefore, with respect to PI and PHI data collection, the risk for individuals is high, while the incentives for organizations are significantly lower. Organizations can collect PI and PHI and combine the data with other data sets obtained through its data supply chain or internet scraping. Then, they can leverage AI and ML to monetize the data and its insights, or they can psychologically influence individuals and the society. Notwithstanding the typical individualized risks associated with PI abuse, such as identity theft, the individualized risks with the COVID-19 pandemic are amplified.[111] The unauthorized disclosure of a positive COVID-19 diagnosis, for example, can subject an individual to societal or familial avoidance or ostracization.[112]

While individuals are more willing to share their PI and PHI given the COVID-19 pandemic[113], technologies, such as contact tracing applications and health monitoring platforms, can collect massive amounts of data. The data can be combined with data sourced from third party data suppliers and internet scraping.[114] Considering this, the risks, such as function creep and data breaches, to individuals is not simply great but is amplified with respect to the pandemic.

---

[105] Dipayan Ghosh, *Don't Give Up on Your Digital Privacy Yet*, SLATE (July 17, 2020), https://slate.com/technology/2020/07/data-privacy-surveillance-law-marketers.html.
[106] *Id.*
[107] *Id.*
[108] *See* IBM SEC. AND PONEMON INST., COST OF A DATA BREACH REPORT (2019) (the report considered the "typical activities" for the discovery of and the response to a data breach to determine the identification and response time. Seventeen industries were included in the study with a sample size of 507—13% of which are based in the United States followed by 9% in India and the United Kingdom. A total of 16 countries or regions were surveyed. For the survey's methodology, *see* 67-73).
[109] *See id.* at 54.
[110] *Id.*
[111] *See generally* Müge Fazlioglu, *Privacy Risks to Individuals in the Wake of COVID-19*, INT'L ASS'N OF PRIVACY PROF'LS (June 2020), https://iapp.org/media/pdf/resource_center/privacy_risks_to_individuals_in_the_wake_of_covid19.pdf.
[112] *See id.* at 5; *See also* SARAH MASLIN NIR, *They Beat the Virus. Now They Feel Like Outcasts*, N.Y. TIMES (May 20, 2020), https://www.nytimes.com/2020/05/20/nyregion/coronavirus-victims-immunity.html (noting COVID-19 survivors in New York faced stigmatization).
[113] Ghose, *supra* note 16, at 26-27.
[114] *See supra* Part I.B.

III. THE CURRENT LEGAL STANDARDS AND JURISPRUDENCE

Having discussed the technologies and data ecosystem, this article turns to the current data privacy, security legal standards, and jurisprudence.

Despite concerns regarding privacy and security in the internet age[115], individuals may trust organizations to use best practices with respect to data privacy and security protocols and legal standards. Although, the willingness to share data during the pandemic increases[116], the question is whether the current regime provides sufficient protections for individuals, which is critically important given the opportunity for organizations to exploit the willingness during the pandemic.

Section A discusses the constitutional protections for individuals provided in the Fourth Amendment of the United States Constitution and state constitutions. Also, Section A discusses statutory protections.[117] Section B details the *reasonable expectation of privacy* standard—the standard frequently used for privacy protections—and it provides a new framework to evaluate privacy expectations and the reasonableness of those expectations. Lastly, Section C explores the shift in privacy expectations caused by the pandemic.

A. Fourth Amendment, Statutory, and State Constitutional Protections

Data privacy and security protections are primarily provided for in the Fourth Amendment and similar bodies of law.[118] These sources of privacy protections are discussed below.

The Fourth Amendment provides that individuals have a right to be secure "in their persons, houses, papers, and effects, against unreasonable searches and seizures . . .."[119] Its purpose is to "safeguard the *privacy* and *security* of individuals" against the arbitrary invasions by government officials.[120] The Framers included the Fourth Amendment in response to the general warrants and writs of assistance of the colonial era that allowed the British to invade and search individuals' homes in an unrestrained manner.[121]

Over time, the Fourth Amendment's search doctrine evolved from a trespass-centric doctrine focused on "constitutionally protected areas" to a person-centric doctrine that protects individuals when individuals seek to preserve their property as private.[122]

---

[115] *See* Brooke Auxier, *How Americans See Digital Privacy Issues amid the COVID-19 Outbreak*, PEW RSCH. CTR. (May 4, 2020), https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/ (finding the majority of Americans are concerned about data privacy and security, yet they do not understand current privacy laws and regulations).

[116] *See generally* Ghose, *supra* note 16, at 26-28.

[117] State statutory protections are out of scope for this article.

[118] Data privacy and security protections are also provided for in case law, state statutes, and federal and state regulations. These are out of scope for this article. The U.S. Constitution provides for privacy protections in other amendments (e.g., Third Amendment's protection against the quartering of soldiers in one's home, and the Fifth Amendment's protection against self-incrimination), but these protections are out of scope because they do not apply to *data* privacy and security; *See* U.S. CONST. amends. III & V.

[119] U.S. CONST. amend. IV.

[120] *Carpenter*, 138 S. Ct. at 2213 (emphasis added).

[121] *Riley*, 573 U.S. at 403.

[122] United States v. Jones, 565 U.S. 400, 405-06, n. 3 (2012); Soldal v. Cook County, 506 U.S. 56, 64 (1992).

Olmstead v. United States is one of the first cases that analyzed the distinction between the two views. The issue in *Olmstead* was whether wiretapping a private phone conversation was within the scope of the Fourth Amendment. Chief Justice Taft, writing for the majority, applied the trespass-centric interpretation of the Fourth Amendment.[123] But in his dissent, Justice Louis Brandeis reasoned the Fourth Amendment to be widely applicable in protecting individuals' personal privacy because "[t]ime works changes [and it] brings into existence new conditions and purposes" for such protections.[124] In 1928, Justice Brandeis recognized that the Court must look beyond the literal meaning of the Fourth Amendment and adopt the person-centric interpretation because technological advancements in surveillance were inevitable.[125]

Eventually, the Supreme Court adopted Justice Brandeis's interpretation in *Katz v. United States*.[126] In *Katz*, the Court provided that the Fourth Amendment protects *people* and not *places*.[127] Justice Harlan's concurrence introduced the *reasonable expectation of privacy* standard that is pervasive throughout privacy and security law today.[128]

More recently, the Court recognized the sensitivity of *data* privacy in *Carpenter v. United States*. The Court provided that "when the Government tracks the location of a cell phone, it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[129] And in *Riley v. California*, at least with respect to the Fourth Amendment, "modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[130] In both cases, the Court set out how modern technologies have great consequences for privacy because the technology has the capability to capture every detail of an individual's life.[131] According to the Court, the capability to collect and store the mass amount of data leads to a reasonable expectation of privacy for the individual (i.e., data subject or user).[132] Additionally, in *United States v. Jones*, Justice Sotomayor specifically noted the sensitivity of location data — stating that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[133]

---

[123] *See* Olmstead v. United States, 277 U.S. 438 (1928).

[124] *Olmstead*, 277 U.S. 438 (1928) (Brandeis, J., dissenting) (The majority held that wiretapping a private individual's phone did not constitute a Fourth Amendment violation because the Fourth Amendment only extended to *physical* invasions of a person's home or property. Justice Brandeis dissented and argued for a broad reading and application of the Fourth Amendment, which is widely adopted today. The majority's opinion in *Olmstead v. United States* was overturned in *Katz v. United States*); *See* Anthony P. Picadio, *Privacy in the Age of Surveillance: Technological Surveillance and the Fourth Amendment*, 90 PA. B. ASS'N Q. 162, 164-65 (2019).

[125] *See* Picadio, *supra* note 124, at 164.

[126] Katz v. United States, 389 U.S. 347 (1967).

[127] *Id.* at 351.

[128] *Id.* at 361 (Harlan, J., concurring); *See infra* Part II.B (further explaining Justice Harlan's *reasonable expectation of privacy* test).

[129] *Carpenter*, 138 S. Ct. at 2218.

[130] *Riley*, 573 U.S. at 393.

[131] *See Riley*, 573 U.S. at 394; *Carpenter*, 138 S. Ct. at 2216-20.

[132] *See, e.g.*, *Riley*, 573 U.S. at 393-98; *Jones*, 565 U.S. at 430 (Alito, J., concurring) (noting that individuals have a reasonable expectation of privacy in the whole of their physical movements).

[133] *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

However, the Fourth Amendment, as with the entire United States Constitution, limits the powers and authorities of the federal government and state governments; the Fourth Amendment limitations apply to the states according to the incorporation doctrine under the Fourteenth Amendment.[134] Accordingly, the Fourth Amendment does not apply to *private* actors, but some state constitutions provide individuals privacy and security protections from both public and private actors.[135] For example, Arizona's constitution provides, "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law."[136] Also, Hawaii's constitution provides, "[t]he right of the people to privacy is recognized and shall not be infringed without a showing of a *compelling state interest*."[137]

In the absence of constitutional privacy and security protections, federal and state statutory protections may apply. For instance, at the federal level, HIPAA applies to PHI,[138] and at the state level, the California Consumer Privacy Act ("CCPA") applies to all PI that any qualified business may collect from an individual.[139]

HIPAA requires covered entities (e.g., health care providers) and their business associates to abide by data privacy, security, and breach notification requirements.[140] Several exceptions may apply to HIPAA's protections. For instance, the following disclosures are permissible: (i) disclosures to public health authorities, (ii) disclosures to individuals who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease, and (iii) disclosures to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.[141]

---

[134] *See Mapp v. Ohio*, 367 U.S. 643 (1961) (fully incorporating the Fourth Amendment's "unreasonable searches and seizures" freedom onto the states via the Fourteenth Amendment).

[135] *See Privacy Protections in State Constitutions*, NAT'L CONF. OF STATE LEGISLATURES (May 11, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (listing eleven states that provide explicit privacy protections in their state constitutions: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, New Hampshire, South Carolina, and Washington).

[136] ARIZ. CONST. art. II, § 8.

[137] HAW. CONST. art. I, § 6 (emphasis added); *see infra* Part II.B (discussing the balancing test of an individual's reasonable expectation of privacy against the state's compelling interest).

[138] The Supreme Court has also recognized that individuals have a reasonable expectation of privacy of their PHI, which supports the general conception that HIPAA recognizes a reasonable expectation of privacy; *See, e.g.*, Ferguson v. City of Charleston, 532 U.S. 67 (2001).

[139] *See* STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 1-23 (2019) (providing an overview of key statutory privacy and security protections, including HIPAA and CCPA).

[140] 45 C.F.R. § 164 (HIPAA's Security and Privacy Rules) (the Privacy Rule limits covered entities' use and sharing of PHI with third parties without valid patient authorization, unless a HIPAA exception applies. The Security Rule requires covered entities to maintain administrative, physical, and technical safeguards to prevent threats or hazards to the security of electronic PHI. And per the data breach notification requirement, known as the Breach Notification Rule, covered entities must, upon the discovery of a data breach, notify affected individuals within sixty calendar days); the Data Breach Notification Rule defines a data breach as the "acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [HIPAA] which compromises the security or privacy of the [PHI]"; a business associate is any entity that, on the behalf of a covered entity, creates, receives, maintains, or transmits PHI.

[141] In respective order: 45 C.F.R. § 164.512(b)(1)(i); 45 C.F.R. § 164.512(b)(1)(iv); 45 C.F.R. § 164.512(j)(1)(i).

CCPA provides some of the most comprehensive data privacy and security protections at a state level in the United States. To a prominent degree, the CCPA provides individuals with the following rights and protections: (i) the right to know what PI is collected, including how and why the PI is collected, (ii) the right to erase or delete one's PI, (iii) the right to opt-out of the sale of one's PI, and (iv) the right not to be discriminated against for exercising one's rights and protections under the CCPA.[142] While California is not alone in providing statutory privacy and security protections for individuals, the CCPA is recognized as one of the country's strongest and most comprehensive regimes.[143]

Between the Fourth Amendment, state constitutions, and federal and state statutory protections, individuals have a "patchwork" of privacy and security protections in the United States.[144] But, none of the foregoing protections sufficiently and effectively protect PI and PHI with respect to the data collected and used in response to the pandemic. Thus, some state legislatures and Congress introduced legislation to protect individuals' PI and PHI, but, at least with respect to Congress, no proposed bill has gained traction.[145]

The common thread amongst the privacy and security protections is the *reasonable expectation of privacy* standard—whether the individual had an objectively reasonable expectation of privacy with respect to the PI or PHI that the individual is claiming to be private and secure. This standard is widely considered the foundational inquiry to any assessment of privacy protections.[146] With constitutional protections, the reasonable

---

[142] CAL. CIVIL CODE § 1798.140(c-o) (CCPA defines PI as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"); *See* Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)*, INT'L ASS'N OF PRIVACY PROF'LS 4-6 (July 9, 2018), https://iapp.org/media/pdf/resource_center/Intro_to_CCPA.pdf (CCPA lists specific rights and protections that are categorized in this article as these four categories. Other rights, protections, and obligations are provided for in the CCPA).

[143] *See id.*; Other states have different forms of data privacy and security protections. For instance, Illinois enacted the Biometric Information Privacy Act ("BIPA") that protects individuals and their biometric data. BIPA continues to generate significant litigation against technology companies including Facebook, Amazon, and Microsoft; *See* ALAN S. WERNICK, *Biometric Information – Permanent Personally Identifiable Information Risk*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/.

[144] *Id.* at 7 (noting that privacy protections for individuals come from a variety of laws that vary considerably in their purpose and scope rather than a single comprehensive law).

[145] *See, e.g.*, *Kansas Introduces the COVID-19 Contact Tracing Privacy Act*, SEC. MAG. (June 9, 2020), https://www.securitymagazine.com/articles/92563-kansas-introduces-the-covid-19-contact-tracing-privacy-act (a bill that aims to protect contact tracing data); *See, e.g.*, Bobbie Johnson, *The US's Draft Law on Contact Tracing Apps Is a Step Behind Apple and Google*, MIT TECH. REV. (June 2, 2020), https://www.technologyreview.com/2020/06/02/1002491/us-covid-19-contact-tracing-privacy-law-apple-google/ (describing The *Exposure Notification Privacy Act*, a bipartisan proposal that would prevent potential abuses by COVID-19 apps). Republican senators introduced the *COVID-19 Consumer Data Protection Act* that would implement protocols regarding the collection, use, and transfer of PI and PHI. Democratic senators introduced the *Public Health Emergency Privacy Act* that would effectively do the same as the Republicans' proposal. But one difference between the two bills is that the *Public Health Emergency Privacy Act* would grant a private right of action.

[146] *See generally* Mark Taylor & James Wilson, *Reasonable Expectations of Privacy and Disclosure of Health Data*, MED. L. REV. (Apr. 25, 2019), https://www.doi.org/10.1093/medlaw/fez009 (while Taylor and Wilson's article focuses on English law, the basis for privacy law in England is similar to the United States. Both regimes rely on the *reasonable expectations of privacy* standard).

expectation of privacy is found throughout Fourth Amendment jurisprudence. With statutory protections, the rights and protections are often, if not always, *based* on the reasonable expectation of privacy standard. For example, one has a reasonable expectation of privacy with respect to one's PHI, and, accordingly, Congress enacted HIPAA to protect the privacy and security of PHI. Statutory protections also *promote* the reasonable expectation of privacy—individuals expect PHI to be protected *because* HIPAA exists today. Because privacy and security protections are based on and promote the reasonable expectation of privacy standard, I turn to a deeper explanation of this standard.

B. Reasonable Expectation of Privacy Standard

The reasonable expectation of privacy standard comes from Justice Harlan's concurrence in *Katz v. United States*.[147] Regarding the Fourth Amendment, courts balance the individual's reasonable expectation of privacy against any legitimate government interest.[148] For PHI specifically, the Supreme Court recognized that individuals have a reasonable expectation of privacy in their healthcare records, and, accordingly, the privacy expectation is generally reflected in HIPAA.[149] Since *Katz*, the Supreme Court has not provided a coherent explanation to what makes a privacy expectation reasonable, and some scholars argue that the Fourth Amendment's jurisprudence is illogical, erratic, and confusing.[150] But more recently, other scholars identified common principles that thread throughout the Court's Fourth Amendment jurisprudence—adding clarification to the *Katz* standard and providing a framework to apply in future matters.[151]

To frame Section B, I first propose the Privacy Expectation Continuum ("Continuum") that visually depicts where an individual's privacy expectations may fall and whether such expectations are reasonable. Next, I explain the reasonable expectation of privacy standard developed by Justice Harlan in *Katz*. I describe several relevant Fourth Amendment doctrines that apply to the COVID-19 pandemic, and I explain various principles that give light to what forms a privacy expectation and how the expectation is reasonable or not. Lastly, I argue that the pandemic shifted the reasonable expectation of privacy with respect to PI and PHI.

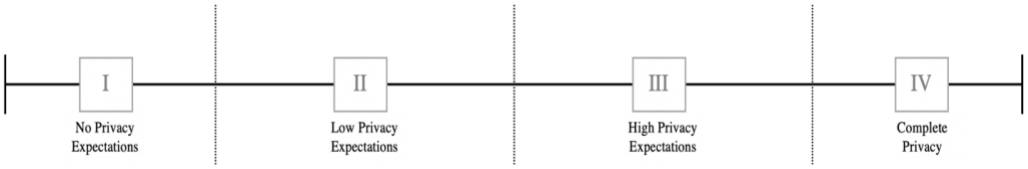
---

[147] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
[148] *See Riley*, 573 U.S. at 385 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).
[149] *See Ferguson*, 532 U.S. at 67.
[150] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504 (2007); *See also* Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 2-3 (2020) (hereinafter "TOKSON'S PRINCIPLES").
[151] *See* TOKSON'S PRINCIPLES, *supra* note 150, at 4 (detailing three principles of the Supreme Court's Fourth Amendment decisions: (i) the intimacy of the place or thing targeted, (ii) the amount of information sought, and (iii) the cost of the investigation); *See also* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139 (2016) (hereinafter "Tokson, *Knowledge*"); *See, e.g.*, Weiyin Hong, *Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective*, J. OF BUS. ETHICS (June 11, 2019), https://www.doi.org/10.1007/s10551-019-04237-1 (testing the Multidimensional Development Theory ("MDT") to the antecedents of internet privacy concern. MDT suggests that an individual's privacy concern is jointly determined by four factors: (i) environmental, (ii) individual, (iii) information management, and (iv) interaction management factors).

Privacy expectations fall on a continuum (Figure 3). I segment the continuum into quadrants where Quadrant I is no expectation of privacy, II is low expectation of privacy, III is high expectation of privacy, and IV is an expectation of complete privacy. Each quadrant is marked with certain characteristics. For example, if an individual has no privacy expectations (Quadrant I), then the individual has no control over the collection, disclosure, storage, or usage of her information. Information in Quadrant II is minimally controlled—the individual maintains *some* privacy expectations, but, otherwise, she willingly discloses the information (e.g., email address). For Quadrant III, the individual controls the information but recognizes the information must be disclosed in a limited capacity in certain situations (e.g., social security number). Finally, for Quadrant IV, the individual expects complete privacy, full control over the information, and strictly limited disclosure or use of the information (e.g., sexual history).

For any information at issue, I consider two points on the Continuum—the objective point and the subjective point. Individuals may place specific categories of information into different quadrants (e.g., sexual history may fall into Quadrant II or III for some individuals) according to their *subjective* privacy expectations. The reasonable person standard determines the objective point. Considering this Continuum, I turn to an explanation of the reasonable expectation of privacy standard before discussing how reasonableness, the *objective* point, is determined.

Figure 3. Privacy Expectations Continuum



In *Katz*, Justice Harlan stated that a Fourth Amendment violation occurs when the person who has "exhibited an actual (subjective) expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"[152] The Supreme Court eventually adopted and condensed Justice Harlan's *Katz* standard—deciding that a search is unreasonable when the government violates an individual's reasonable expectation of privacy.[153] The Court has inconsistently applied and explained the reasonable expectation of privacy standard in the cases since *Katz*.[154]

Despite its inconsistencies, the Court has established several doctrines that it applies with some regularity. First, the third-party doctrine provides that an individual has no reasonable expectation of privacy with her information that she turns over or exposes to third parties.[155] For instance, an individual cannot reasonably expect her call log to be

[152] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
[153] *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 9 (1968) (holding that a person is to be free from unreasonable government intrusion whenever an individual harbors a reasonable expectation of privacy).
[154] *See* TOKSON'S PRINCIPLES, *supra* note 150, at 7-8.
[155] *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).

private because the service provider sees this information.[156] Here, the third-party doctrine categorically places information turned over to third parties into Quadrant I despite an individual personally believing her information falls into a higher quadrant.

While the third-party doctrine is still considered good law today, Justice Sotomayor and many legal scholars advocate for the Court to revisit the doctrine because the doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[157]

However, the Court has retreated from a broad application of the third-party doctrine.[158] In *United States v. Miller*, the Court broadly applied the third-party doctrine in holding that the individual does not have a reasonable expectation of privacy with respect to PI held by third parties when the information is limited in scope and intrusion[159] But unlike *Miller*, in *Carpenter*, the Court stopped short of broadly applying the third-party doctrine to PI that can reveal highly private personal affairs.[160] Unlike in *Miller*, where bank records reveal a limited scope of personal information, in *Carpenter*, cell phone geolocation data reveals highly personal information such as political affiliations, socialization habits, frequently visited locations, etc.[161] *Carpenter*'s limit on the third-party doctrine turned on the scope of the information and level of intrusion.

The level of intrusion or invasion is the second general "principle" that the Court regularly applies.[162] The general rule is that the more intrusive or invasive the action (i.e., search) taken, the more likely the action would infringe on the individual's reasonable expectation of privacy.[163] The information at issue in *Miller* were bank records—the Court held that bank records could only reveal *some* personal information.[164] However, in *Carpenter*, the information at issue—the cell phone geolocation data—revealed significantly more personal information.[165] In other words, the data in *Carpenter* was more intrusive than the data in *Miller*.

The third relevant doctrine addresses technologically enhanced searches. In *Kyllo v. United States*, law enforcement used a heat detection device to penetrate the walls of a

---

[156] *See, e.g.*, United States v. Miller, 425 U.S. 435, 442-43 (1976).

[157] *Jones*, 565 U.S. at 416-17 (Sotomayor, J., concurring) (stating "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties [because] [t]his approach is ill suited to the digital age . . . .").

[158] *See, e.g.*, *Carpenter*, 138 S. Ct. at 2206 (holding that individuals have a reasonable expectation of privacy with respect to cell phone geolocation tracking data because this data can reveal a great deal of PI).

[159] *See generally Miller*, 435 U.S. at 440-43 (holding that an individual does not maintain a reasonable expectation of privacy with respect to bank records).

[160] *See Carpenter*, 138 S. Ct. at 2206.

[161] *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (geolocation data may reveal "familial, political, professional, religious, and sexual associations."); S*ee Carpenter*, 138 S. Ct. at 2217-18 (the Court declined to extend the third party doctrine because "[g]iven the unique nature of cell phone location records . . . when the Government tracks the location of a cell phone it achieves near perfect surveillance . . . .").

[162] *See, e.g.*, Birchfield v. North Dakota, 136 S. Ct. 2160 (2016) (holding that a warrantless breath test of an intoxicated individual is reasonable, but a warrantless blood draw is an unreasonable search because blood draws are significantly more intrusive); some scholars may not consider the level of intrusiveness as a doctrine—hence, for this article, it is considered a general "principle" in the Court's jurisprudence.

[163] *See, e.g.*, *id.*; Schmerber v. California, 384 U.S. 757 (1966) (holding that a blood sample to test one's blood alcohol content is a search within the Fourth Amendment).

[164] *See supra* note 161.

[165] *Id.*

home to "see" inside.[166] While the device did not physically intrude into the individual's home, the technology enabled the law enforcement's..[167] Here, *Kyllo* would fall into Quadrant III.

The fourth relevant doctrine is the common law trespass doctrine, which came before Justice Harlan's reasonable expectation of privacy standard.[168] In short, an individual maintains a reasonable expectation of privacy with respect to her property. Historically, the Court applied the Fourth Amendment's protection and a person's expectation of privacy to *physical property* (e.g., an individual's home).[169] But today, an individual's reasonable expectation of privacy applies to the *person*, not just the person's property.[170]

In *Jones*, the Government attached a GPS monitoring device to Jones' automobile, and the Court held, "[t]he Government usurped Jones' property [and property interest in Jones' automobile] for the purpose of conducting surveillance on him . . . ."[171] However, if Jones consented to the GPS tracking, then Jones would not have had a reasonable expectation of privacy.[172] Justice Alito concurred in *Jones*, but he recognized the common-law trespass doctrine and the reasonable expectation of privacy standard may be ineffective or unworkable given the development and advancement of new technologies; electronic surveillance does not physically intrude on a person's property and individuals may relax their expectations of privacy as a tradeoff with the convenience that new technologies provide.[173]

Now, the question becomes *how* the Court determines the reasonableness of an expectation of privacy (i.e., the objective point on the Continuum). Legal and constitutional scholars recently identified certain principles and frameworks that the Court typically applies to privacy claims.

An analysis of the more than forty Fourth Amendment cases from the Supreme Court shows three emerging principles, for which the interaction between these principles

---

[166] Kyllo v. United States, 533 U.S. 27 (2001).

[167] *Id.* at 33-34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' . . . constitutes a search" within the terms of the Fourth Amendment); PICADIO, *supra* note 124, at 167.

[168] *Jones*, 565 U.S. at 409 ("the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

[169] *See, e.g., Olmstead*, 277 U.S. at 438 (holding that the Fourth Amendment was not applicable because, while the Government wiretapped a phone, there was no physical entry into the home); Olmstead was later overturned as the Supreme Court evolved the Fourth Amendment's protections from a property-centric approach to a person-centric approach.

[170] *See, e.g., Katz*, 389 U.S. at 351; *See supra* Part II.C and note 123 and accompanying text; Alderman v. United States, 394 U.S. 165, 176 (stating that the Supreme Court did not move away from the property-centric approach to the Fourth Amendment protections, but rather, the Court extended the protections to the person and their private conversations).

[171] *Jones*, 565 U.S. at 413 (Sotomayor, J., concurring).

[172] *See id.* at 409 ("the specific question [in *Knotts*] was whether the installation [of a tracking beeper] '*with the consent of the original owner*' constitute[d] a search or seizure . . . [w]e held not." (quoting United States v. Karo, 468 U.S. 705, 707 (1984)).

[173] *Id.* at 426-27 (Alito, J., concurring) ("[T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance [because it] has traditionally required a physical touching of property. . . New technology may provide increased convenience or security *at the expense of privacy*, and many people may find the tradeoff worthwhile.").

is key: (i) the intimacy of the place or thing targeted by the government (the "Intimacy Principle"), (ii) the amount of information sought (the "Amount Principle"), and (iii) the cost of the investigation (the "Cost Principle").[174]

Regarding the Intimacy Principle, if the information sought is highly personal or sensitive in nature, then the surveillance is more likely to infringe on an individual's privacy expectations.[175] Like in *Carpenter*, where the Court determined the individual had a reasonable expectation of privacy, the cell phone data was intimate because it revealed a broad picture of the individual's life—aligning with the intrusiveness principle.[176] Here, Carpenter maintained a higher subjective point on the Continuum, and the Court agreed that the objective point aligned with Carpenter's privacy expectations.

For the Amount Principle, the more extensive and longer in duration, the more likely the surveillance will infringe on an individual's privacy expectations.[177] For example, the Court determined that long-term monitoring of an individual's automobile using a GPS tracker infringed on the individual's privacy expectations.[178] And in *Carpenter*, the Court stressed its concern regarding the dangers of collecting voluminous amounts of data.[179]

With respect to the Cost Principle, if the government can gather large amounts of data at a relatively low cost, the surveillance is more likely to infringe on an individual's privacy expectations.[180] In *Jones*, Justice Alito noted that low-cost surveillance techniques, which are more prevalent given technological advancements, have eroded structural barriers that, historically, made government surveillance difficult and costly.[181] For instance, in *Carpenter*, the cell phone data provided the government with intimate PI with little to no effort and cost—the government simply asked the cell phone service provider for the records.[182]

Carpenter provides the best example of the three principles and how these principles interact. The government sought cell phone records that revealed detailed location data over a long period of time (Intimacy Principle).[183] These records were voluminous (Amount Principle).[184] And obtaining these records was of little to no cost to the government (Cost Principle).[185] While the Court does not explicitly frame its analysis using these principles, in *Carpenter* and other cases, the Court *applies* or *considers* these principles when analyzing the issue. These principles aid the Court in determining the objective point on the Continuum.

---

[174] TOKSON'S PRINCIPLES, *supra* note 150, at 13 (Tokson does not name the three principles. I name the principles for this article).
[175] *Id.* at 15 ("The more intimate the place or thing targeted by the police for investigation, the more likely such investigation is to infringe the privacy of the affected person or persons.").
[176] *See Carpenter*, 138 S. Ct. at 2217-18; *supra* note 161 and accompanying text.
[177] TOKSON'S PRINCIPLES, *supra* note 150, at 18.
[178] *Jones*, 565 U.S. at 430 (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").
[179] *Carpenter*, 138 S. Ct. at 2217-18; TOKSON'S PRINCIPLES, *supra* note 150, at 19 ("[The Court] repeatedly emphasized the dangers that such a volume of data posed to a citizen's privacy . . . .").
[180] TOKSON'S PRINCIPLES, *supra* note 150, at 23.
[181] *Jones*, 565 U.S. at 429 (Alito, J., concurring); TOKSON'S PRINCIPLES, *supra* note 150, at 24.
[182] *See* TOKSON'S PRINCIPLES, *supra* note 150, at 25.
[183] *Carpenter*, 138 S. Ct. 2212.
[184] *Id.* at 2209.
[185] TOKSON'S PRINCIPLES, *supra* note 150, at 25.

But as Justice Alito recognized in *Jones*, technological advancements may erode individuals' reasonable expectations of privacy.[186] And while an on-point case has not come before the Court, advancements in technologies may *erode* the privacy expectations *even if* the facts are similar to *Carpenter* (i.e., intimate PI collected at mass volumes at a relatively low cost). Why? Because an individual's privacy expectations are a function of what the individual knows and experiences.[187] This "formula" can be shown as follows, where EoP is the expectation of privacy, K is knowledge, and E is experience ("EoP Formula"):

$$\boldsymbol{EoP = f(K + E)}$$

For example, in *United States v. Forrester*, the Ninth Circuit Court of Appeals determined that the individual *knowingly* exposed PI (his IP address) when the individual visited a website.[188] More specifically, the court concluded that individuals "should know that this information is . . . provided to [i]nternet service providers."[189] Here, the Court considered *knowledge* (Forrester knew he disclosed the information) and *experience* (individuals *should know* information is shared with internet service providers given their experiences with websites).

The EoP Formula holds true when there is a lack of knowledge or a different set of experiences. In a situation like *Carpenter*, it is not common knowledge for someone to know the intimacy of the data collected in her cell phone records.[190] With cell phone data, courts have held that there is a reasonable expectation of privacy because it is unlikely that most people (i) *know* or *should know* the amounts of intimate data collected by cell phone providers, and (ii) do not have sufficient personal experiences (e.g., working for a cell phone service provider) to have such knowledge.[191]

Even if an individual holds a reasonable expectation of privacy, the individual's privacy expectations may be set aside if the government's interest is sufficiently compelling. Under the special needs doctrine, the government can demonstrate a "special need" to justify a search where the individual has a reasonable privacy expectation.[192] For example, the Supreme Court upheld *suspicionless* drug tests as a condition of

---

[186] *See Jones*, 565 U.S. at 429; TOKSON'S PRINCIPLES, *supra* note 150, at 23.
[187] Tokson, *Knowledge*, *supra* note 151, at 149.
[188] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007); Tokson, *Knowledge*, *supra* note 151, at 150.
[189] *Forrester*, 512 F.3d at 510 (9th Cir. 2007).
[190] *See* Tokson, *Knowledge*, *supra* note 151, at 158-64 (explaining cell phone location information [or CSLI, the same data at issue in *Carpenter*], a Third Circuit Court of Appeals decision held that it is unlikely that individuals know cell phones and cell phone providers collect and store massive amounts of intimate data).
[191] *See generally id.*
[192] *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663-65 (1995) (finding it lawful to drug test student athletes where there was some evidence of athletes using marijuana because student athletes can be role models to other students).

employment[193] or for participation in public school activities.[194] And in *Skinner v. Railway Labor Executives Ass'n*, the Court upheld the drug testing program of railroad employees because the government had a "special need" in identifying impaired performance that could injure the passengers or the public.[195] In short, the government's role in protecting public health and safety may be a sufficient justification for a suspicionless search under the special needs doctrine, as the Court showed in *Skinner*.

From an economic rationale, the government's interest in protecting public health and safety may rest in the value of a human life, among other reasons. National Public Radio's *Planet Money* podcast explained the general rule that any federal safety regulation must pass a cost-benefit test—if the costs of the regulation (e.g., money) exceed the benefits (e.g., lives saved), the regulation is rejected.[196] Historically, economists considered the *cost of death* in the cost-benefit analysis.[197] But today, economists consider the cost of death plus the cost that individuals place on themselves *for the value of their lives*.[198] Kip Viscusi, a risk and uncertainty economist at Vanderbilt University, calculates the value of a "statistical life" today to be $10 million.[199]

For perspective, Viscusi calculated the cost-benefit of shutting down the economy in order to slow the spread of COVID-19; he assumed one million lives were saved from the economic shutdowns,[200] multiplied by the $10 million per statistical live, and he arrived at $10 trillion as the "benefit" in the cost-benefit analysis.[201] And considering $10 trillion is approximately half of the United States GDP, this "benefit" estimate means that "in order to justify completely opening businesses back up, the economy would need to lose half of its value—" the basic and conservative calculation results in an extremely high cost *if there was not a shutdown*.[202]

Here, with respect to COVID-19, the government's compelling interest is saving lives and protecting public health. Viscusi placed a dollar figure on *how much* the government's interest is in protecting the public health—it would cost $10 million in

---

[193] *See, e.g.*, Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 769 (1989) (holding that the government had a sufficient "special need" when requiring applicants to take a drug test for federal employment positions); S*ee also* Wendy Mariner, *Reconsidering Constitutional Protection for Health Information Privacy*, 18 U. PA. J. CONST. L. 975, 1022-23 (describing the special needs doctrine).

[194] *See, e.g.*, Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. V. Earls, 536 U.S. 822, 836-37 (2002) (holding that the school district had a sufficient "special need" in requiring students participating in extracurricular activities to take a drug test); *see also* Mariner, *supra* note 193, at 1022-23.

[195] Skinner v. Railway Labor Executives Ass'n, 489 U.S. 602, 633 (1989).

[196] *Planet Money, Lives vs. The Economy*, NAT'L PUB. RADIO, at 04:35 (Apr. 15, 2020), https://one.npr.org/?sharedMediaId=835571843:858418568.

[197] *Id.* at 05:13.

[198] *Id.* at 10:12-12:05 ("[P]eople are putting a dollar value on their own lives all the time based on the jobs that they do. How risky they are, and how much money they're willing to accept, in wages, for those risky jobs.").

[199] *Id.* at 21:31 (Viscusi's cost model takes the average cost across the entire labor market, considering factors such as the likelihood of death on the job and how much extra money workers demand for that risk of death).

[200] *Id.* at 22:00 (Viscusi used the one-million-lives-saved assumption because (i) President Donald Trump publicly stated that one million lives were saved, and (ii) epidemiologists stated that it could be as high as two million lives saved. Viscusi chose the conservative estimate).

[201] *Id.* at 22:09 (the "benefit" is saving $10 trillion in the *value of lives* where the "cost" in the cost-benefit analysis is the economic impact (e.g., the economic contraction) of the shutdowns).

[202] *Id.* at 22:23 (emphasis added).

economic value for each life lost.[203] Applying this figure to the privacy discussion, this means that while individuals may have a reasonable expectation of privacy with respect to their PI and PHI, even during the pandemic, the government's compelling interest (here, demonstrated by the economics of "the value of life") override or set aside privacy protections. Further, given this compelling interest, individuals are more willing to share their PI and PHI in the interest of public health.[204] This marks a shift in privacy expectations and the reasonableness of those expectations, which I turn to next.

C. The Shift in the Privacy Expectations and Reasonableness

Prior to the COVID-19 pandemic, PHI was generally considered private and protected, and for the most part, PHI still is.[205] However, in only a few months' time, the pandemic shifted privacy expectations of PHI, and by doing so, the reasonableness of privacy expectations. This Section C describes (i) the shift in privacy expectations, and (ii) the newfound reasonable expectation of *disclosure* during the pandemic. For this section, this article presumes that (i) the more sensitive a category of information is considered, the more likely individuals desire to keep that category of information private, and (ii) the more willing individuals are to share information, the less private individuals consider that information to be.

Americans consistently and reliably considered their health data as one of the most sensitive categories of data.[206] Respondents to a 2014 survey rated health data as the second highest category of information (the first being their social security numbers) with respect to the privacy and sensitivity of the data.[207] More than half of adults considered their health data to be "very sensitive" in nature.[208] Moreover, most adults consider their health data to be *just as sensitive* as the content of their private phone conversations.[209] Per these survey responses, health data falls into Quadrants III or IV on the Continuum, depending on the data's specifics.

Similar levels of sensitivity apply to other types of information. Half of adults consider their geolocation data to be very sensitive.[210] And approximately 25% of adults

---

[203] *See supra* note 201 and accompanying text.
[204] Ghose, *supra* note 16, at 28.
[205] *See* discussion *supra* Part II.A.
[206] *See* Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RSCH. CTR. (Nov. 12, 2014), https://www.pewresearch.org/wp-content/uploads/sites/9/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (the survey was conducted between January 10-27, 2014, with a sample size of 607 adults, all of whom were 18 years of age or older. A total of 1,537 panelists were invited to respond, of which 935 responded, and 607 agreed to join the survey panel. Four separate surveys regarding the "current issues, some of which relate to technology." The sampling error is ±4.6% at a 95% level of confidence); *See also* Gallup Org., *Public Attitudes Toward Medical Privacy*, INST. FOR HEALTH FREEDOM (Sept. 2000) (detailing a survey from 2000 that shows similar levels of concern regarding the privacy of health data. The survey is presented here to show that privacy concerns regarding health data has remained relatively constant over time).
[207] *Id.* at 7 (I use the term "healthcare data" for this article, but Pew Research Center described this type of information as "state of your health and the medications you take" in the survey).
[208] *Id.* at 32.
[209] *Id.* at 33.
[210] *Id.* at 34.

consider their search history, religious views, political views, and who their friends are to be considered very sensitive, while 8% of adults consider their purchasing habits very sensitive.[211]

The COVID-19 pandemic shifted the *willingness* of individuals to share these sensitive categories of information. As of April 2020, 84% of adults said that they would be more willing to share their health data to combat the spread of COVID-19, and 58% of adults said that they would be willing to share their geolocation data.[212] Furthermore, approximately two-thirds of adults stated that they would be willing to install an app on their devices to help slow the spread of the pandemic, even if the app collected geolocation and health data.[213]

In comparing the pre- and during-pandemic surveys, there is a shift in the willingness to share data and information, which suggests individuals have lowered their sensitivity to sharing their health data.[214] This may be attributable to several factors, for which, unfortunately, little to no data exists to confirm or invalidate.[215] These factors could include an individual's self-interest in mitigating the effects of the pandemic (e.g., reopening businesses), a sense of "doing their part" in combating the pandemic, a recognition of the benefits in sharing the data, or a recognition of the level of risk associated with sharing the data.[216]

Here, the pandemic shifted both the objective and subjective points on the Continuum. The pre-pandemic survey responses suggest individuals would place their health data into Quadrants III or IV (the subjective point). Recognizing a shift in privacy expectations has occurred, to provide a possible explanation as to why this shift occurred, I turn back to the three principles and the formula to determine the reasonableness of privacy expectations (objective point).[217]

First, the Intimacy Principle remains constant for the health and geolocation data—nothing changed regarding how intimate the data sets are for individuals prior to the pandemic versus during the pandemic.[218]

Second, for the Amount Principle, this article assumes that the amount of health data remains constant.[219]

---

[211] *Supra* note 206, at 37.
[212] Ghose, *supra* note 16, at 3.
[213] *Id.*
[214] It is difficult to determine whether the shift in willingness to share PHI is permanent because no post-pandemic data exists. As of November 2020, the pandemic is ongoing.
[215] *See supra* note 214 and accompanying text.
[216] These factors are speculative and non-exhaustive. Some factors may be temporary (i.e., only last during the pandemic and may reverse an individual's willingness to share their PHI post-pandemic) or permanent (i.e., continuing post-pandemic and have permanently changed an individual's willingness to share their PHI). An example of a temporary factor is the "doing their part" in combating the pandemic (once the pandemic ends, there no need for an individual to "do their part" in combating the virus). A permanent factor could be the recognition of the level of risk (an individual considering the sensitivity of her PHI is lower because she sees more benefit than risk associated with sharing the data post-pandemic; the trade-off calculation changed).
[217] *See* discussion *supra* Part II.B and note 151.
[218] *See id.*
[219] *See id.*

Third, the Cost Principle may explain the shift.[220] Here, the Cost Principle extends beyond a monetary cost. The tradeoff calculation for individuals changed—a majority of adults believe that preventing the spread of COVID-19 (benefit) is more important than protecting people's privacy with respect to their PHI (cost).[221] In other words, individuals see the increased benefit or reduced risk in sharing the data under a traditional cost-benefit analysis. However, this calculation changes if the data is released publicly—during-pandemic survey data shows that 61% of adults are uncomfortable with public disclosure of their PHI.[222] This suggests there is still some expectation of privacy as individuals are still uncomfortable with public disclosure, but a shift in those privacy expectations occurred because most individuals rate the pandemic response as more important than protecting people's privacy. In other words, the objective point—what is reasonable to society—has not shifted entirely to the left of the Continuum (no expectation of privacy). If an individual were to claim the pre-pandemic privacy expectation with respect to her health and geolocation data, it would likely be unreasonable because this shift occurred—society, or at least a portion thereof, now believes disclosure of PHI to combat COVID-19 is beneficial.

Applying the EoP Formula, both knowledge and experience changed because of the pandemic.[223] Here, the individual's personal knowledge changed; individuals know, or should know, that geolocation data can and will likely be used for contact tracing purposes. With the public attention COVID-19 has generated, society better understands what contact tracing is, its value to combating the spread of COVID-19, and what data contact tracing requires.[224] And individuals have had experiences in combating the virus (e.g., wearing masks, social distancing, etc.) and feeling the pandemic's global impact (e.g., air travel changes and interruptions, economic contractions, etc.). These changes—in individual knowledge and experiences—provide an explanation for the change in individuals' privacy expectations; more individuals are willing to share their PHI given the pandemic.[225]

---

[220] *See id.*

[221] Grant Buckles, *Americans Rank Halting COVID-19 Spread Over Medical Privacy*, GALLUP (May 15, 2020), https://news.gallup.com/poll/311015/americans-rank-halting-covid-spread-medical-privacy.aspx (of those surveyed, 39% responded that they would prioritize protecting people's medical privacy over preventing the spread of COVID-19, and 61% answered that they would prioritize the latter over the former).

[222] Lucy Simko, et al., *COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences* 10, (May 8, 2020) (Univ. of Wash., Working Paper), https://seclab.cs.washington.edu/wp-content/uploads/2020/05/contact-tracing-user-privacy.pdf.

[223] *See supra* Part II.B and note 187.

[224] *See, e.g.*, ED. BD., *America Could Control the Pandemic by October. Let's Get to It.*, N.Y. TIMES (Aug. 8, 2020), https://www.nytimes.com/2020/08/08/opinion/sunday/coronavirus-response-testing-lockdown.html; Benjamin Lesser, et al., *Local Governments 'Overwhelmed' in Race to Trace U.S. COVID Contacts*, REUTERS (Aug. 4, 2020), https://www.reuters.com/investigates/special-report/health-coronavirus-tracing/; BUCKLES, *supra* note 221; Chas Kissick, et al., *What Ever Happened to Digital Contact Tracing?*, LAWFARE (July 21, 2020), https://www.lawfareblog.com/what-ever-happened-digital-contact-tracing.

[225] *See* Buckles, *supra* note 221 and accompanying text; *See also* Jennifer Steinhauer & Abby Goodnough, *Contact Tracing Is Failing in Many States. Here's Why.*, N.Y. TIMES (July 31, 2020), https://www.nytimes.com/2020/07/31/health/covid-contact-tracing-tests.html (contact tracing applications have not been successfully deployed. The several factors that may explain why the United States has not successfully deployed contact tracing include (i) the number of people, (ii) the delay in getting test results back, and (iii) the wide community spread of COVID-19).

Given this change in the privacy expectations of PHI, in certain situations, individuals may have a reasonable expectation of *disclosure*.[226] In certain situations, individuals *expect* the disclosure of their PHI. Two situations where individuals are likely to have a reasonable expectation of disclosure are: (i) for public health and safety purposes, and (ii) for customer experience purposes associated with modern technology. Individuals may expect their PHI data to be transmitted to public health authorities, contact tracing applications, and the like for the reasons previously described.[227] Further, individuals may expect the sharing of their PHI between organizations because modern technology (e.g., user interface and experience design) have set expectations regarding the use, functionality, and convenience of technology.[228] For instance, individuals get frustrated if they must answer the same medical-related questions repeatedly—they expect the PHI to be shared to avoid the tedious repetition or friction in the customer experience.[229]

Justice Harlan's *reasonable expectation of privacy* standard is the basis for privacy law—under both the Fourth Amendment and statutory protections, such as HIPAA.[230] While not explicitly described by the Supreme Court, the Court considers several principles that are generally used to establish whether a claimed infringement of an individual's privacy expectations is reasonable.[231] While individuals and society reasonably expect their PI and PHI to be private, the COVID-19 pandemic shifted those privacy expectations.[232] To illustrate this shift, I turn to a case study in Part III.

IV. A CASE STUDY: THE PANDEMIC'S EFFECT ON THE LAW

Organizations that bring together large numbers of individuals (e.g., employers, universities, etc.), in efforts to return to some level of normalcy and to protect individuals whom they are responsible for, have implemented or are implementing various programs and initiatives using health surveillance technology.[233] For example, Ernst & Young and the International Association of Privacy Professionals surveyed organizations to better understand the pandemic's impact and how organizations are responding to it from a

---

[226] *See generally* Taylor, *supra* note 146, at 453.
[227] *See supra* Part II.B (Intimacy, Amount, and Cost Principles and the EoP Formula).
[228] *See generally* Taylor, *supra* note 146, at 453.
[229] *Id.*
[230] *See supra* Part II.A.
[231] *See supra* Part II.B.
[232] *See supra* Part II.C.
[233] *See, e.g.*, TRUSTARC PRIVACY INTELLIGENCE, *Managing Employee Privacy in the Face of COVID-19*, TRUSTARC (Mar. 19, 2020), https://trustarc.com/blog/2020/03/19/managing-employee-privacy-in-the-face-of-covid-19/ (describing inquiries it received regarding employee privacy matters); Philip Gordan, et al., *Frequently Asked Questions on Workplace Privacy and COVID-19*, LITTLER MENDELSON P.C. (Mar. 31, 2020), https://www.littler.com/publication-press/publication/frequently-asked-questions-workplace-privacy-and-covid-19 (discussing legal issues regarding PHI and employee privacy); Jenn Abelson, et al., *At College Health Centers, Students Battle Misdiagnoses and Inaccessible Care*, WASH. POST (July 13, 2020), https://www.washingtonpost.com/investigations/2020/07/13/college-health-centers-problems/?arc404=true (describing efforts that universities took or are taking); Letter from Doug McMillon, et al., Chairman, Bus. Roundtable, to Vice President Michael R. Pence (Apr. 24, 2020), https://s3.amazonaws.com/brt.org/Business-Roundtable-GuidelinesforReturningtoWork-2020.04.24.pdf (a letter from Fortune 500 chief executives belonging to the Business Roundtable calling for national standards to protect workers and customers).

privacy and security perspective.[234] Over 50% of employers have collected some level of PHI from their employees about symptoms, and 60% of organizations identified that they are keeping records of employee diagnosed with COVID-19.[235] Universities have been and are at the forefront of the response—implementing health and safety initiatives for their students, employees, and visitors.[236]

To better illustrate the shift in the privacy expectations with respect to PI and PHI, and the reasonableness of those expectations, this Part III details the efforts by Arizona State University ("ASU") as a case study. I select ASU as a case study because (i) it is a public institution that (ii) has three primary constituent groups—students, staff and faculty, and visitors—each presenting a unique set of challenges. Part III is not intended to be an exhaustive analysis of the legal or constitutional issues related to ASU's initiatives or the initiatives of other universities. Rather, Part III synthesizes the information presented in Parts I and II regarding the technologies and the legal standards to present a better understanding of how the rapidly emerging health surveillance technologies, traditional jurisprudence, and legal standards interplay.

This Part III considers ASU's contact tracing, case management, and health monitoring platforms. I describe the technology ASU deployed, discuss the possible data supply chain design, evaluate the data privacy and security risks, and apply the current legal standards and jurisprudence.

Before the pandemic, ASU deployed and utilized an electronic health record system and practice management system ("HRS/PMS") from Point and Click Solutions, Inc. ("PointNClick") for its university-wide campus health services.[237] At the start of the pandemic, PointNClick added new features and capabilities to its platform to enable its customers to respond to the global health emergency.[238] For example, PointNClick added a contact tracing feature that, if a student tests positive for COVID-19, the HRS/PMS will automatically place the person in a contact tracing queue that will enable the university to take additional actions to prevent an outbreak.[239]

For staff and faculty case management and contact tracing, ASU deployed Salesforce.com's Work.com solution ("Work").[240] Work's contact tracing capability

---

[234] *See* Müge Fazlioglu, *Privacy in the Wake of COVID-19: Remote Work, Employee Health Monitoring and Data Sharing*, ERNST & YOUNG & INT'L ASS'N OF PRIVACY PROF'LS (May 2020), https://iapp.org/resources/article/iapp-ey-report-privacy-in-wake-of-covid19/ (the target population for the survey included in-house privacy and IT professionals. Respondents were solicited via IAPP's website, emails, and social media accounts. Responses were collected between April 8-20, 2020, and 933 respondents completed the survey).

[235] *Id.* at iv.

[236] *See, e.g.*, *Novel Coronavirus*, ARIZ. STATE UNIV., https://eoss.asu.edu/health/announcements/coronavirus (last visited Aug. 12, 2020); *COVID-19 News & Resources*, STAN. UNIV., https://healthalerts.stanford.edu/ (last visited Aug. 12, 2020); *COVID-19*, UNIV. OF TEX. AT AUSTIN, https://coronavirus.utexas.edu/ (last visited Aug. 12, 2020); *NYU Returns: 2020-2021 Academic Year*, N.Y.U., https://www.nyu.edu/life/safety-health-wellness/coronavirus-information.html (last visited Aug. 12, 2020).

[237] *See, e.g.*, POINT AND CLICK SOLUTIONS, https://www.pointandclicksolutions.com/ (last visited Aug. 15, 2020).

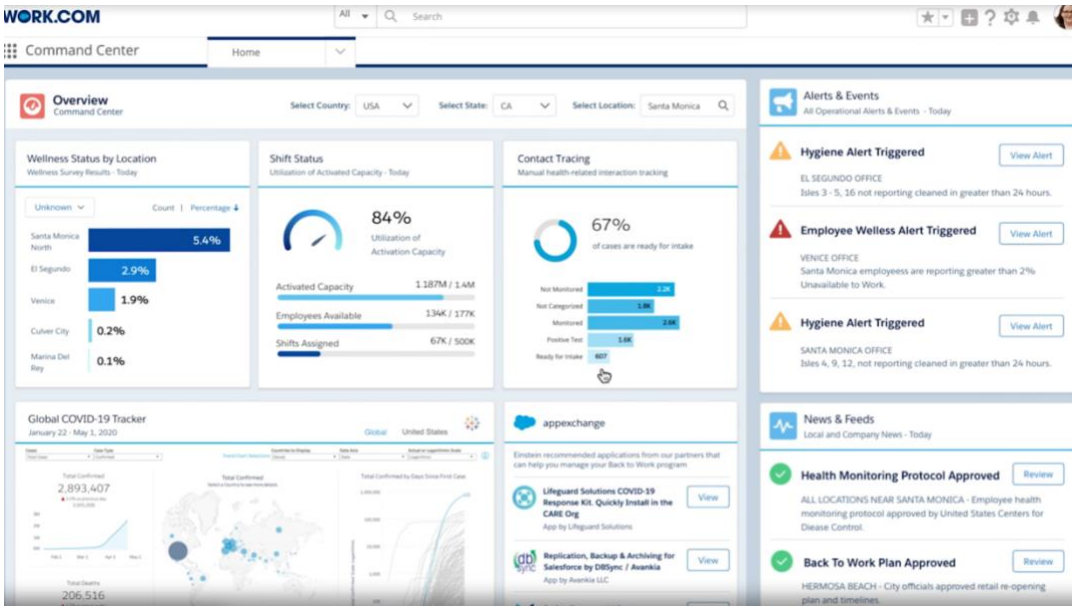
[238] *COVID-19 Response*, POINT AND CLICK SOLUTIONS, https://www.pointandclicksolutions.com/covid-19-response (last visited Aug. 15, 2020).

[239] *Id.*

[240] *See, e.g.*, WORK.COM, https://www.salesforce.com/work/?sfdc-redirect=219 (last visited Aug. 15, 2020).

enables its customers to "manually trace interactions across employees, customers, meetings, and locations to identify possible points of transmission."[241] Work allows people managers to track their employees' COVID-19 test results, symptoms, visited locations, event attendance, etc., and it allows employees to track their own contacts via dashboard visualizations (Figure 4).[242]

Figure 4: Work Dashboard Screenshot[243]



Furthermore, ASU's University Technology Office embedded a white label health monitoring platform, SAFE, into its mobile application (Figure 6).[244] The university requires all students, staff, and faculty to complete a daily health check, powered by SAFE, using the ASU mobile application; the daily health check asks whether the individual is experiencing any symptoms or has come in contact with anyone who has experienced symptoms of COVID-19.[245] Failure to complete the daily health checks may result in the suspension of access to university systems, tools, and resources.[246]

---

[241] *Protect Your Workforce with Manual Contact Tracing Solutions*, WORK.COM, https://www.salesforce.com/products/contact-tracing/overview/?d=cta-body-promo-112 (last visited Aug. 12, 2020).

[242] Salesforce.com, *Work.com Demo*, SALESFORCE.COM (Aug. 15, 2020), https://www.salesforce.com/form/contact-tracing/demo/?d=cta-header-90.

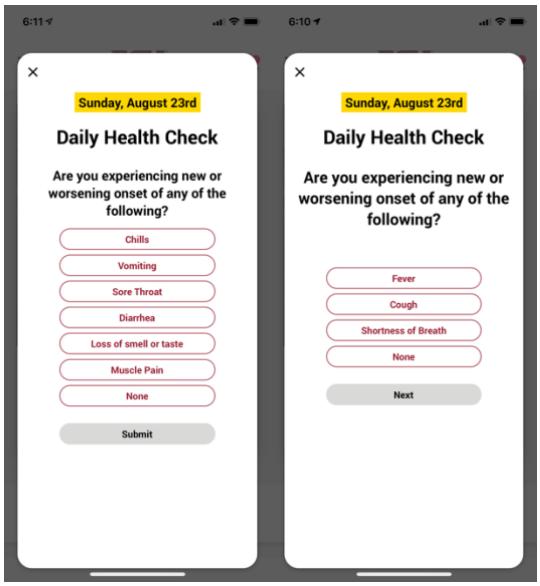
[243] *Id.* at 0:19.

[244] *See* Part I.A.; *See also* SAFE HEALTH SYSTEMS, INC., *supra* note 35 and accompanying text. Individuals can also complete the daily health checks via an ASU web application or by phone, Mark S. Searle, *Required Daily Health Check*, ASU HEALTH SRVCS (Aug. 11, 2020), https://eoss.asu.edu/health/announcements/coronavirus.

[245] Searle, *supra* note 244.

[246] *Id.*

Figure 6: SAFE Embedded into ASU's Mobile Application



The three platforms, PointNClick, Work, and SAFE integrate with other ASU systems and tools.[247] These integrations require the transmission of PI or PHI between them for proper functionality. Both PointNClick and Work require individuals—students, staff, and faculty—to provide PI, such as locations visited; this is user-inputted data. SAFE, via the ASU mobile application, requires individuals to provide PHI—symptom information; this is also user-inputted data.

For queried data, ASU sources data from both internal and external parties. ASU sources internal data from other systems and tools to enable the platforms.[248] For information security purposes, ASU sources IP-data from external data suppliers for identity verification.[249] Moreover, ASU's systems and tools will autogenerate PI that is used across the network of systems and tools for various purposes, such as information security and campus safety.[250]

---

[247] *See, e.g.*, Christine L. Borgman, *Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier*, 33 BERKELEY TECH. L.J. 365, 368 (2018) ("As universities outsource more computing systems and services . . . they relinquish . . . control." I make certain assumptions regarding the integration of systems and tools for this article. These assumptions are based on professional knowledge of information technology systems and tools, including information security best practices and processes); for example, both systems integrate with ASU's single-sign-on ("SSO"). The SSO data is transmitted between ASU systems and tools to authenticate the user's identity. A more thorough description of ASU's system and tool integrations are out of scope for this article.

[248] *E.g.*, ASU's student records management system transmits a student's educational program to determine if the student is an on-campus or online student. On-campus students must complete the daily health check.

[249] *E.g.*, ASU sources the geolocation of a user's IP address to determine whether the individual seeking access to the network is truly the owner of the credentials used to login to the system or tool.

[250] *E.g.*, ASU will autogenerate a login register—tracking where, when, and for how long a user is logged into a system.

SAFE requires user-inputted data. But while PointNClick and Work were deployed for contact tracing purposes, these systems require more than the user-inputted data. Considering the totality of the PI and PHI collected, stored, and used by ASU, whether user-inputted, queried, or autogenerated data, there are two risks worth detailing: the risk of (i) a data breach, and (ii) function creep.

ASU, and likely every university, is at risk for a data breach because it collects, stores, and uses vast amounts of PI, PHI, and other data.[251] Universities are the third highest sector for data breaches in the United States because they maintain in-depth and diverse data sets regarding its students, staff, faculty, and research.[252] They have already seen state-sponsored cyberattacks—China sponsored a cyberattack against American universities in an attempt to steal intellectual property and research related to the pandemic.[253] In April 2019, hackers stole PI of students, staff, and faculty from Georgia Institute of Technology, and in 2017, Washington State University was breached and 1.1 million individuals' PHI was compromised.[254] The pandemic-related increase in the collection, storage, and use of PI and PHI and the rapid deployment of the technologies have increased the data breach risk.

But the risks extend beyond data breaches and the theft of PI and PHI for individuals. PointNClick, Work, and SAFE collect PI and PHI that was not previously collected by ASU—contacts, events attended, daily symptom checks, COVID-19 status, etc. While ASU may not retain the data indefinitely, other organizations deploying similar efforts may, and considering the likelihood that the data will be retained by the organization after the pandemic, the potential for misuse and abuse multiplies when the organization aggregates the data and applies ML/AI to the data sets.[255] For example, while the data is collected for the health monitoring of students, staff, and faculty, the data could be used for university research purposes.[256]

Under Fourth Amendment jurisprudence and normal circumstances, this data collection and usage would be unlawful or unconstitutional. While these platforms do not automatically collect geolocation data, like in *Carpenter* and *Riley*, the intimacy and amount of data (geolocation and health monitoring PI and PHI) would make the data collection and usage initiatives unconstitutional because "it [would] achieve near perfect surveillance."[257] If an automated geolocation feature were activated on SAFE, for example, the contact tracing data would reveal highly sensitive information about ASU's students, staff, and faculty because it would generate "a precise, comprehensive record of a person's

---

[251] *See* Borgman, *supra* note 247, at 368.
[252] *Id.* at 405.
[253] *See, e.g.*, Ellen Nakashima & Devlin Barrett, *U.S. Accuses China of Sponsoring Criminal Hackers Targeting Coronavirus Vaccine Research*, WASH. POST (July 21, 2020), https://www.washingtonpost.com/national-security/us-china-covid-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0_story.html.
[254] *10,000 Breaches Later: Top Five Education Data Breaches*, IDENTITY THEFT RES. CTR. (Aug. 17, 2020, 7:04 PM), https://www.idtheftcenter.org/10000-breaches-later-top-five-education-data-breaches/.
[255] *See* Borgman, *supra* note 247, at 401.
[256] Borgman, *supra* note 247, at 400-01.
[257] *Carpenter*, 138 S. Ct. at 2218.

public movements", similar to the comprehensive GPS monitoring that occurred in *Jones*.[258]

But in the age of COVID-19, this data collection and usage should not surprise students, staff, and faculty. While ASU has communicated its objectives with respect to PointNClick, Work, and SAFE to students, staff, and faculty, privacy expectations remain, albeit these expectations shifted since the start of the pandemic. Before the pandemic, students, staff, and faculty likely would have been concerned with the university's data collection because survey data suggests the overall privacy concerns of health data.[259] Before the pandemic, the objective and subjective points on the Continuum likely would have been in Quadrants III or IV, but the pandemic shifted these points to Quadrant II. Individuals have lower subjective privacy expectations.[260] And given the knowledge of and experience with the pandemic, the objective point—the reasonableness of privacy expectations—is lower. If an individual were to claim a higher expectation of privacy on the Continuum—a subjective point in Quadrant III or IV—with respect to her pandemic-related PHI, such expectations would now be unreasonable because the reasonable person has a lower privacy expectation.[261]

Regardless of where the objective and subjective points fall on the Continuum, the compelling government interest in protecting the public health and safety would set aside the privacy expectations under the special needs doctrine.[262] ASU, as a public university, is subject to the Fourth Amendment as a public actor, and like in *Skinner*, where the drug testing program's intent was to protect public safety, ASU's COVID-19 programs have the same intent. Moreover, under HIPAA, ASU, as both a covered entity and a business associate, could invoke the public health exemptions.[263]

The special needs doctrine would also apply to any common law trespass claim under the Fourth Amendment. Under the common law trespass doctrine, an individual could claim a Fourth Amendment violation because the university effectively requires students, staff, and faculty to download the ASU mobile application to their personal phones.[264] By effectively forcing the download and installation of a health monitoring application onto one's personal property, ASU would be unconstitutionally conducting a search via its monitoring. While the claim would have merit under normal circumstances, during the pandemic, the special needs doctrine would set this claim aside, even without considering the subjective and objective points on the Continuum.

For public actors, like universities, contact tracing and health monitoring applications and platforms pose privacy and security risks for individuals. Despite the risks of function creep and data breaches, these applications and platforms are lawful and constitutional

---

[258] *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); ASU has not activated the automated geolocation feature as of November 2020.
[259] *See* Madden, *supra* note 65, at 7 and accompanying text.
[260] *See* Part II.C.; *See also* Madden, *supra* note 206 and accompanying text.
[261] *See* Part II.C.; *See also* Ghose, *supra* note 212 and accompanying text.
[262] *See supra* Part II.B.
[263] *See supra* Part II.A.
[264] A common law trespass claim would not apply to ASU-provided devices, only personal devices. ASU allows for the completion of the daily health checks via a web portal or by phone. Students, staff, and faculty are not required to download the ASU mobile application. A common law trespass claim would likely consider these alternative methods of completion.

because the pandemic shifted privacy expectations and the reasonableness of those expectations—the subjective and objective points on the Continuum. Moreover, they are lawful and constitutional under the government's compelling interest in protecting the public health and safety.

V. THE INEFFECTIVENESS AND UNWORKABILITY OF THE REASONABLE EXPECTATION OF PRIVACY STANDARD AND RECLAIMING THE RIGHT TO PRIVACY

The pandemic revealed the ineffectiveness and unworkability of the reasonable expectation of privacy standard. The shift in the objective and subjective points on the Continuum show that privacy expectations are not constant—they change over time and in response to personal and societal experiences and knowledge. This is one of two faults with the reasonable expectation of privacy standard; it presumes that privacy expectations remain constant over time, and that a reasonable person maintains a well-informed and development set of privacy expectations.[265] But the *need* for privacy is constant.

Section A explains the faults and why the standard will not protect individuals' data privacy and security. And Section B proposes a new legal standard that would protect data privacy and security regardless of shifting expectations.

A. The Ineffective and Unworkable Katz Standard

The COVID-19 pandemic illustrated the ineffectiveness and unworkability of the reasonable expectation of privacy standard. The shift in the objective and subjective points on the Continuum show that privacy expectations are not constant—they change over time. Yet, the *need* for privacy does not disappear. Moreover, there are two faults with the reasonable expectation of privacy standard: it presumes that (i) privacy expectations remain relatively constant over time, and (ii) a reasonable person maintains a well-informed and developed set of privacy expectations.[266] This Section A explains these faults and why the standard will not protect individuals' data privacy and security over time.

The *need* for privacy is constant. Even though the subjective and objective points shifted, the *risks* associated with the unauthorized access, use, or dissemination of PI and PHI have not changed since the pandemic began. For instance, the pandemic did not suddenly change the risks associated with unauthorized use of one's geolocation data—malicious actors prior to and during the pandemic can use the geolocation data to identify one's social connections, political affiliations, and the like.[267] The need for privacy remains constant because the inherent value of PI and PHI to the individual is unchanged—the value of one's PHI did not change with the onset of the pandemic.

The reasonable expectation of privacy standard does not incorporate the *values* and *risks* of PI and PHI. The reduction of subjective privacy expectations given the pandemic, under the reasonable expectation of privacy standard, any unauthorized or malicious access, use, or dissemination of PI or PHI may not result in a privacy violation or infringement in the eyes of the law.[268] In *Carpenter*, intimate cell phone location data was considered so private that obtaining such data requires a warrant by law enforcement.[269]

---

[265] *See Jones*, 565 U.S. at 427 (Alito, J., concurring).
[266] *Id.*
[267] *Jones*, *supra* note 133, at 415.
[268] *See* Buckles, *supra* note 221.
[269] Grande, *supra* note 30.

The shift in the objective point on the Continuum, the same intimate data collected and used for contact tracing may not be considered as sensitive as it was in *Carpenter*. But it is the exact same data.

Justices Alito, Ginsburg, Breyer, and Kagan recognized the reasonable expectation of privacy standard assumes stability in privacy expectations; in *Jones*, the concurrence stated that the reasonable expectation of privacy standard is flawed because it "rests on the assumption that this hypothetical person has a well-developed and stable set of privacy expectations."[270] But the pandemic introduced instability—the objective and subjective points shifted.

As technology advances, privacy expectations change—leading to significant changes in "popular attitudes" regarding privacy.[271] The prevailing "popular attitude" may differ from person to person—this shows the fault in that the reasonable expectation of privacy standard presumes a well-informed set of privacy expectations. Judges are apt to confuse their own privacy expectations with those of the reasonable person under *Katz*.[272] Judges may have different knowledge and sets of experiences that shape their placement of the objective point on the Continuum. Since the reasonable expectation of privacy is a function of knowledge and experience, what is knowledgeable to a well-educated judge is significantly different than the ordinary person.[273]

This prompts the question as to whether the reasonable expectation of privacy will diminish to a point where there is *no expectation* of privacy. Likely not, but nonetheless, the value and risks remain. Accordingly, the need for privacy protections remain. This calls for a new legal standard—the right to control.

B. Reclaiming the Right to Privacy with a New Legal Standard and Legislative Action

There are two priorities to reclaim the right to data privacy and security. The first is to replace the reasonable expectation of privacy test from *Katz* with a more robust standard. The second is comprehensive forward-thinking data privacy and security legislation from Congress. This Section B proposes a new standard—the right to control—to replace the ineffective and unworkable reasonable expectation of privacy standard. Further, this section implores Congress to enact comprehensive data privacy and security legislation to protect individuals, their PI, and their PHI.

The *right to control* would be the effective and workable standard to replace the reasonable expectation of privacy standard. It would ask whether an individual's right to control his data, its privacy, and its security was violated or infringed.

Unlike the reasonable expectation of privacy standard, where objective and subjective privacy expectations may wane over time, the right to control standard would not weaken when privacy expectations shift because the standard relies on *tangible control*, not intangible and fluctuating expectations. As Justice Alito said in *Jones*, the reasonable

---

[270] *Jones*, 565 U.S. at 427 (Alito, J., concurring).
[271] *Id.*
[272] *Id.*
[273] *See* Part II.B and the EoP Formula.

expectation of privacy standard presumes stability, but under a right to control standard, stability would be a non-issue because an individual gets to determine the control of her own data.[274] The reasonable expectation of privacy considers the external factors—what are the reasonable expectations of privacy of an objective person—where knowledge and experience weigh heavily on the determination. The right to control standard would not consider these external factors because it would be solely dependent on whether the individual's right to control his data was infringed. The right to control would be an affirmative civil right not subject to the reasonable person objective standard.

Further, the right to control standard incorporates and appreciates the inherent value of the PI or PHI—individuals get to control their data based on the value they place on their information. For example, as previously mentioned, individuals may have different levels of sensitivity regarding their sexual history—some would place their sexual history on Quadrant IV and others would place it in Quadrant II or III on the Continuum.[275] Under the right to control standard, the individual reclaims the right to determine where a category of her data falls on the Continuum for herself unlike under the reasonable expectation of privacy standard where the data collector makes the determination subject to any constitutional or statutory protections.

Changing the standard is necessary, but not sufficient in comprehensively protecting individuals' PI and PHI. Congress must pass comprehensive data privacy and security legislation. Congress recognizes the need to do so. Prior to and during the pandemic, members of Congress proposed various data privacy and security bills.[276] But these privacy and security bills fail to gain traction in Congress.[277]

Congress cannot turn to the industry to self-regulate or provide proposals for data privacy and security legislation for two reasons. First, as idealistic companies age, companies exchange governmental regulation for governmental protection. For instance, with Facebook, Mark Zuckerberg invites government regulation because such regulation would protect Facebook's monopoly on social media.[278] This is no different than Theodore Vail, the former president of AT&T, submitting to government regulation in the 1910s that allowed AT&T to dominate for decades.[279]

Second, while organizations may self-regulate, the number of high-profile data privacy lapses and data breaches show a private market failure.[280] The fundamental issue with self-regulation is the conflict of interest that exists—the regulators are the regulated.[281] Here,

---

[274] *Jones*, 565 U.S. at 427 (Alito, J., concurring).
[275] *See* Part II.B.
[276] Tony Romm, *Members of Congress to Unveil Bipartisan Bill to Regulate Contact-Tracing Apps, Fearing Potential Privacy Abuses*, WASH. POST (June 1, 2020), https://www.washingtonpost.com/technology/2020/06/01/contact-tracing-congress-privacy/ (explaining the *Exposure Notification Privacy Act* proposed by Sen. Maria Cantwell and other senators).
[277] David Uberti, *Coronavirus Privacy Bills Hit Roadblocks in Congress*, WALL ST. J. (June 15, 2020), https://www.wsj.com/articles/coronavirus-privacy-bills-hit-roadblocks-in-congress-11592213400 (describing the partisan differences that prevent privacy bills from advancing in Congress).
[278] Franklin Foer, *What Big Tech Wants Out of the Pandemic*, THE ATL. (July/August 2020), https://www.theatlantic.com/magazine/archive/2020/07/big-tech-pandemic-power-grab/612238.
[279] *Id.*
[280] Wayne Unger, *Reclaiming Our Right to Privacy by Holding Tech Companies Accountable*, RICH. J.L. & TECH. (forthcoming 2020).
[281] *Id.*

actually protecting individuals' PI and PHI by improving privacy and security practices (e.g., prohibiting the processing and dissemination of data) conflicts with the regulators' (the organizations themselves) source of revenue.[282] More simply, it is counterintuitive for organizations to improve their privacy and security capabilities if the improvements negatively impact their revenue and profits.[283]

Therefore, Congress needs to act comprehensively. While this article does not exhaustively list all of the rights, protections, and obligations that must be created with Congressional action, the legislation should preempt the states to prevent a patchwork of varying levels of protection.[284] It must include a private right of action that will allow individuals to seek redress, but the private right of action should be limited by procedural filters, such as an opportunity to cure an alleged violation, to avoid unnecessary and meritless litigation.[285] And the legislation should be data-subject-centric—meaning that the drafting must protect individuals and their data, not an organization's revenue or profits. A data-subject-centric approach can be achieved by establishing duties of loyalty and care onto organizations for the benefit of individuals.[286] Lastly, the legislation must recognize the three types of data (user-inputted, queried, and autogenerated) and data supply chains to effectively provide data privacy and security protections end-to-end.

By changing the legal standard from the reasonable expectation of privacy to the right to control, individuals reclaim data privacy and security. Congress must act in passing comprehensive data privacy, and security legislation to create effective and necessary protections because the need for personal privacy and security is always present.

---

[282] Unger, *supra* note 280.
[283] *Id.*
[284] Cameron Kerry, et al., *Bridging the Gaps: A Path Forward to Federal Privacy Legislation*, BROOKINGS INST. (June 3, 2020), https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/.
[285] Unger, *supra* note 280 at 5-6.
[286] *See* Kerry, *supra* note 284.

CONCLUSION

The COVID-19 pandemic has thrusted health surveillance technologies into the spotlight, and with the technologies, the data privacy and security issues that come with them. The collection, use, and dissemination of PI and PHI is necessary to combat the virus and slow the spread. But as organizations move to deploy these technologies, we must consider the types of data and existence of data supply chains to fully understand the totality of privacy and security risks.

With the totality of understanding, we can evaluate the effectiveness and workability of current legal standards and protections. The pandemic revealed the ineffectiveness and unworkability of the reasonable expectation of privacy standard because the objective and subjective points on the Continuum shifted. To truly protect individuals' data privacy and security, the legal standard must change to a right to control, and Congress must act to pass comprehensive data privacy and security legislation because "invasions upon [an individual's] privacy, subject [the individual] to mental pain and distress, far greater than could be inflicted by mere bodily injury."[287]

[287] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 196 (1890).