



2024

## Unavoidability in U.S. Privacy Law

Laura M. Moy


*Georgetown University Law Center*, [laura.moy@georgetown.edu](mailto:laura.moy@georgetown.edu)

This paper can be downloaded free of charge from:  
<https://scholarship.law.georgetown.edu/facpub/2580>  
<https://ssrn.com/abstract=4577608>

---

Science & Technology Law Review, Vol. 25, No. 1, 2023, Pp. 56-108.

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.  
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [Intellectual Property Law Commons](#), [Legislation Commons](#), and the [Privacy Law Commons](#)

---

THE COLUMBIA  
SCIENCE & TECHNOLOGY  
LAW REVIEW

---

VOLUME 25

STLR.ORG

FALL 2023

---

## ARTICLE

## UNAVOIDABILITY IN U.S. PRIVACY LAW

Laura M. Moy\*

*Why is U.S. privacy law structured the way it is, with a series of sectoral laws rather than a cross-sectoral law or laws? Why does U.S. privacy law protect information shared in certain contexts—such as information shared with an attorney, a healthcare provider, or a financial provider—rather than particular types of information? One possibility is that sectoral laws apply to contexts in which people typically share highly “sensitive” information containing intimate secrets or with the potential to harm them financially or psychologically.*

*But this Article argues that there is something else at play—that in fact, an under-discussed and underappreciated factor has been a key consideration throughout the history of U.S. privacy law: the unavailability of information sharing. Tracing the development of several areas of sectoral U.S. privacy law over time, this Article shows that as society changed and contexts emerged in which individuals increasingly found they could not avoid sharing information about themselves with other parties, policymakers repeatedly responded by ratcheting up the privacy protections for information shared in those specific contexts.*

*Taking the discussion of unavailability into the modern era, this Article ties the tradition of unavailability consideration in U.S. privacy law to lawmakers’ current struggle to craft comprehensive privacy legislation. Recent years have seen*

---

\* Associate Professor of Law, Georgetown University Law Center. The author is grateful to Julie Cohen, Eric Null, Paul Ohm, and Tanina Rostain for feedback and guidance on this article. The author also thanks Kendra Albert, Kevin Arlyck, Chinmayi Arun, D.R. Jones, Woody Hartzog, Blake Reid, Neil Richards, David Super, David Vladeck, and countless other friends and colleagues for exceedingly helpful workshop facilitation, participation, and feedback at the 2020 Privacy Law Scholars Conference, a 2022 faculty workshop at Georgetown Law, and a 2023 talk at the Information Society Project at Yale Law School. Special thanks also to the staff and students of the Communications & Technology Law Clinic for their patience, support, and engagement on many of the topics discussed in this article.

*widespread recognition that the sectoral approach is no longer adequate in the modern information economy. But legislators struggle to decide whether it is sufficient to focus on facilitating individuals' control over their data—as U.S. privacy law historically has strived to do—or whether the law should more directly restrict the use of data in certain ways or for certain purposes. This Article argues that the current privacy legislation struggle, and the types of innovative legislative provisions being proposed, can be better explained with the aid of unavailability analysis*

|      |   |     |
|------|---|-----|
| I.   | INTRODUCTION.....   | 57  |
| II.  | DEFINING AND CLASSIFYING UNAVOIDABILITY .....                                   | 59  |
|      | A. <i>Unavoidable services</i> .....  | 60  |
|      | B. <i>Unavoidable providers</i> .....   | 61  |
|      | C. <i>Unavoidable transactions</i> .....  | 63  |
|      | D. <i>Practical unavailability</i> .....  | 64  |
| III. | UNAVOIDABILITY AS EVER-PRESENT IN THE HISTORY OF U.S. PRIVACY LAW ..            | 65  |
|      | A. <i>Unavailability in medical privacy</i> .....                               | 66  |
|      | B. <i>Unavailability in Attorney-Client Privilege and Confidentiality</i> ..... | 71  |
|      | C. <i>Unavailability in Communications Privacy</i> .....                        | 73  |
|      | D. <i>Unavailability in Financial Privacy</i> .....                             | 76  |
|      | E. <i>Unavailability in Fourth Amendment Third-Party Doctrine</i> .....         | 81  |
|      | F. <i>Unavailability in Educational Privacy</i> .....                           | 84  |
|      | G. <i>Unavailability in Section 5 of the FTC Act</i> .....                      | 87  |
| IV.  | POLICYMAKERS' HISTORICAL PATTERN FOR ADDRESSING UNAVOIDABILITY ...              | 89  |
|      | A. <i>Rationales for protecting information shared unavoidably</i> .....        | 89  |
|      | B. <i>How policymakers have protected information shared unavoidably</i> .....  | 94  |
| V.   | PRECIPITOUS UNAVOIDABILITY AND THE CURRENT LEGISLATIVE DILEMMA ....             | 95  |
|      | A. <i>Precipitous unavailability in the digital era</i> .....                   | 96  |
|      | B. <i>The failure of the incumbent policy framework</i> .....                   | 105 |
| VI.  | CONCLUSION .....  | 107 |

## I. INTRODUCTION

Why is U.S. privacy law structured the way it is, with a series of sectoral laws rather than a cross-sectoral law or laws? Why does U.S. privacy law typically protect information shared in certain contexts—such as information shared with an attorney, a healthcare provider, or a financial provider—rather than particular types of information? One possibility is that these are the contexts in which highly private “sensitive” information most often is shared, information that reveals people’s most intimate secrets or that could be used to do them a great deal of harm.

But this Article argues that there is something else at play—that in fact, an under-discussed and underappreciated factor has been a key consideration throughout the history of U.S. privacy law: the *unavoidability* of information sharing. Tracing the development of several areas of sectoral U.S. privacy law over time, this Article shows that as society changed and contexts emerged in which individuals increasingly found they could not avoid sharing information about themselves with other parties, policymakers repeatedly responded by ratcheting up the privacy protections for information shared in those specific contexts. This is why the U.S. protects information in particular contexts, but lacks a cross-sectoral baseline privacy law.

Recent years have seen widespread recognition that the sectoral approach is no longer adequate in the modern information economy. But legislators struggle to decide whether it is sufficient to focus on facilitating individuals' control over their data—as U.S. privacy law historically has strived to do—or whether the law should more directly restrict the use of data in certain ways or for certain purposes. Indeed, at the same time that Congress has considered a multitude of traditional “privacy” bills, it also has generated draft legislation with innovative new provisions to directly address a number of problems that are linkable to the collection, processing, and use of personal data, such as data-driven discrimination, dark patterns, algorithmic opacity, and the display of harmful online content to kids and teens.

Some have argued that provisions to address some of these problems ought to be included in privacy legislation. Others have argued that privacy legislation should be limited in scope to giving individuals rights to control, access, and delete some categories of “personal” data, and that other data-driven harms—even if they are unquestionably data-driven—are outside the scope of what privacy law is supposed to do.

This Article argues that in fact, these innovative new policy proposals can be explained as the logical next step in the centuries-old story of U.S. privacy law's efforts to address information shared unavoidably. The Article makes two claims.

The first claim of this Article is that throughout the history of U.S. privacy law, policymakers have recognized the degree of unavoidability in information sharing as relevant in determining what policies ought to apply to the information shared. A careful exploration of the privacy tradition through several different contexts in roughly chronological order illustrates the longstanding relevance of unavoidability in information policymaking. Examining the history of medical confidentiality, attorney-client privilege and confidentiality, Section 5 of the FTC Act, Fourth Amendment Third-Party Doctrine, educational privacy, financial privacy, and communications privacy reveals that unavoidability was a key consideration for policymakers all along. Indeed, in many of these contexts, the impetus for policymakers to establish new privacy protections was that society changed over time and contexts emerged in which it became less avoidable for individuals to share information. As mentioned above, unavoidability alone is and has not been dispositive—it has been considered alongside a handful of other factors that are

already well understood to play an important role when determining privacy or data protection standards, including the norms and expectations of information subjects, the degree of sensitivity of the information shared, and the severity of direct and tangible harms, such as identity theft.

The second claim of this Article is that policymakers' current struggle to define the appropriate scope and goals of privacy legislation can be better explained with the aid of unavailability analysis. In the digital era with ubiquitous computer-aided analysis and cheap storage, a great deal of information sharing—across many sectors—has become unavoidable for the average person. The precipitous recent growth in unavoidable information sharing matches the same historical pattern of unavailability that has triggered policymakers to act in the past, and the innovative provisions cropping up in legislative proposals seek to deliver on the same goals that have motivated past policymakers grappling with unavoidable information sharing.

## II. DEFINING AND CLASSIFYING UNAVOIDABILITY

Before evaluating the underappreciated historical role of unavailability in U.S. privacy law, “unavailability” must be defined. For the purposes of this Article, the definition of unavailability is straightforward. An unavoidable information sharing is one that the information subject cannot prevent from occurring. Another way of formulating unavailability is an individual sharing information under conditions that either lack voluntariness or knowledge. It is worth acknowledging that one natural extension of this argument could be that unavailability is the same as a lack of consent because knowledge and voluntariness are both widely accepted as necessary for consent to exist. Therefore, critical deficits in these areas could be interpreted as rendering consent impossible.<sup>1</sup>

This Article does not, however, explore whether for every information sharing posited as unavoidable, consent would legally be nonexistent and impossible. Rather, the question this Article focuses on is whether, as a matter of policy, U.S. law has applied and/or should apply heightened protections to situations in which an individual cannot reasonably avoid the information sharing. Compromised knowledge and voluntariness, as discussed in consent theory, are useful to guide this exploration. In the historical examination of U.S. privacy law that follows, discussion of both voluntariness and knowledge is common.

There are at least four ways in which information sharing may be unavoidable and thus, as this Article explains, historically receiving and arguably deserving of policymakers' concerted attention. First, unavoidable information sharing may occur when an individual uses a service so important that availing oneself of it lacks

---

<sup>1</sup> NANCY S. KIM, *CONSENTABILITY: CONSENT AND ITS LIMITS* 9 (2019). A few years ago, Evan Selinger and Woodrow Hartzog analyzed knowledge and voluntariness—specifically, within the context of the framework set forth by Kim—to argue persuasively that facial surveillance likely is in consentable and that, therefore, moratoria against this technology are warranted. *See generally* Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 *LOYOLA L. REV.* 101, 105–109 (2019).

voluntariness. Second, unavoidable information sharing may occur when only one or a few providers exist in a particular context, so an individual's patronage of a particular provider thus lacks voluntariness. Third, unavoidable information sharing may occur when, under the circumstances, an individual finds that a specific transaction lacks voluntariness. Fourth, unavoidable information sharing may occur when information is withheld from an individual about how their information will be collected and/or used, thus rendering the information sharing unavoidable as a practical matter.

These four categories of unavoidability are conceptually distinct but rarely occur in isolation. Concrete examples within each category will serve to animate them. For each category of unavoidability, it is also worth examining *for whom* an information sharing may be unavoidable if it is not unavoidable for all.

#### A. Unavoidable services

When an individual shares information about themselves as a necessary part of accessing and/or using an essential service, the information sharing generally lacks voluntariness, and the information sharing is thus unavoidable.<sup>2</sup> Consider the words of the Privacy Protection Study Commission, established by the Privacy Act of 1974, discussing the appropriate level of protection for the records that individuals share with medical providers, banks, and credit card issuers: “While in theory these relationships are voluntary, in reality an individual today has little choice but to establish them as he would be severely, and perhaps insurmountably, disadvantaged if he did not.”<sup>3</sup>

The vast majority of people partake, at least to some extent, of multiple services generally recognized as essential, such as housing, healthcare, and public utilities. Since the establishment of the Universal Declaration of Human Rights in 1948, the United Nations has asserted that food, clothing, housing, medical care, necessary social services, and education are important enough to be protected as fundamental rights.<sup>4</sup> In the past decade, internet access has joined the list of services generally accepted as essential.<sup>5</sup> The United Nations Human Rights Council now recognizes

---

<sup>2</sup> See ALAN WERTHEIMER, COERCION 36 (1987) (discussing cases in which have been held to have been made under duress and stating, “utilities provide an essential service for which there is no alternative supplier, and it is often unreasonable to expect the customer to refuse to give in to a utility's demand and sue later in an attempt to recover.”).

<sup>3</sup> Privacy Protection Study Commission, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 20 (1977).

<sup>4</sup> G.A. Res. 217 (III) A, Universal Declaration of Human Rights, Art. 25 and 26 (Dec. 10, 1948).

<sup>5</sup> See U.N. Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, ¶ 2, U.N. Doc. A/HRC/17/27 (May 16, 2011) (stating that “[t]he Special Rapporteur believes that the Internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies,” and asserting that “facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States.”).

a right to freedom of expression online.<sup>6</sup> Indeed, some have argued that broadband should be recognized and regulated as a utility.<sup>7</sup>

Although some essential services are needed by virtually everyone, others are needed only by some, owing to their particular circumstances. For example, there are certain types of assistance that are not always needed by everyone, but when an individual is unemployed, sick, or disabled, assistance services are essential, and information shared in the pursuit thereof is shared unavoidably. Indeed, the United Nations considers assistance for people who are unemployed, sick, or disabled to be fundamental rights.<sup>8</sup> Khiara Bridges has written extensively on the unavoidability of information sharing by people of low-income, particularly women. Bridges opens her book on *The Poverty of Privacy Rights* with the transcript of an invasive psychosocial assessment administered to a mother seeking state-assisted prenatal care and notes, “[T]his is a painfully personal conversation that privately insured pregnant women can and, absent unique circumstances, usually do avoid.”<sup>9</sup> In contrast, economically disadvantaged mothers must share private information in order to receive benefits needed to provide their children with basic necessities.<sup>10</sup>

That the essential nature of a service diminishes the voluntariness of sharing information in that context has been recognized for a long time across multiple areas of law. This is why in contract law, the doctrine of economic duress generally recognizes duress in situations involving individuals’ agreement to unreasonable terms for utilities.<sup>11</sup>

### B. Unavoidable providers

When a provider is overwhelmingly dominant and an individual then must share information with that provider because they require the service the provider offers, that information sharing lacks voluntariness and is unavoidable. Some specific providers with overwhelming dominance or ubiquity are unavoidable to a large number of individuals. As noted above, categories of unavoidability rarely occur in isolation, and there are many examples of unavoidable providers offering unavoidable services.

The unavoidability of a provider may be different for different people. In some locations, people may find that there is only one available provider for a particular service. For example, many people in the United States live in places where there

---

<sup>6</sup> Human Rights Council Res. 47/16, The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/47/16 (July 13, 2021); see Catherine Howell & Darrell M. West, *Commentary: The Internet as a Human Right*, BROOKINGS INST. (Nov. 7, 2016), <https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/>.

<sup>7</sup> See, e.g., Susan Crawford, *Why Broadband Should Be a Utility*, BROADBAND COMMUNITIES, Mar.–Apr. 2019, at 50, <https://www.bbcmag.com/law-and-policy/why-broadband-should-be-a-utility>.

<sup>8</sup> G.A. Res. 217 (III) A, *supra* note 4, at Art. 25 and 26.

<sup>9</sup> KHIARA BRIDGES, *THE POVERTY OF PRIVACY RIGHTS* 4 (2017).

<sup>10</sup> *Id.* at 9–10.

<sup>11</sup> See John Dalzell, *Duress by Economic Pressure I*, 20 N.C. L. REV. 237, 243 (1942).

is only one available provider for high-speed internet. According to a 2020 analysis from the Institute for Local Self-Reliance, at that time “at least 83.3 million Americans [could] only access broadband through a single provider.”<sup>12</sup>

People of lower income may also find that they have fewer choices than their wealthier counterparts when it comes to selecting a provider of any given service, simply because they cannot afford more expensive options. For example, when choosing a mobile device, some people may find that they lack the resources to have a meaningful choice of mobile operating system—due to financial constraints, they feel they have no choice but to purchase an inexpensive device, which is likely to be an Android device.<sup>13</sup>

In addition, people in marginalized communities historically have faced exclusionary treatment by certain providers, thus diminishing the options available to them and increasing the likelihood that a transaction is unavoidable. For example, in 1959 when Henrietta Lacks needed to see a specialist for a gynecologic problem that turned out to be cervical cancer, she had no choice but to go to Johns Hopkins. As Rebecca Skloot explains in *The Immortal Life of Henrietta Lacks*, Ms. Lacks and her husband went to Hopkins because in the Jim Crow era, that was the only major hospital close enough to go to that would treat a Black woman.<sup>14</sup> Skloot explains, “when black people showed up at white-only hospitals, the staff was likely to send them away, even if it meant they might die in the parking lot.”<sup>15</sup> In the context of her unavoidable interaction with a care provider at Johns Hopkins, Ms. Lacks shared her health information and genetic material with the institution, which resulted in countless repeated violations of her and her family’s privacy over the ensuing decades. One hundred years after Ms. Lacks’s birth, the editorial board of *Nature* magazine wrote, in a piece calling for better medical privacy standards, “for decades after her death, doctors and scientists repeatedly failed to ask her family for consent as they revealed Lacks’s name publicly, gave her medical records to the media, and even published her cells’ genome online.”<sup>16</sup>

---

<sup>12</sup> Christopher Mitchell & Kate Kienbaum, *Report: Most Americans Have No Real Choice in Internet Providers*, INST. FOR LOCAL SELF-RELIANCE (Aug. 12, 2020), <https://ilsr.org/report-most-americans-have-no-real-choice-in-internet-providers/>.

<sup>13</sup> See, e.g., Jordan Palmer, *iPhone vs. Android: Which Is Better for You?*, TOM’S GUIDE, Jan. 5, 2022, <https://www.tomsguide.com/face-off/iphone-vs-android> (“The vast majority of the world’s smartphones run Android, and because so many companies build Android handsets, they’re available at every price range. . . . The same cannot be said for iPhones, which historically have been expensive at launch, only to come down in price after successive generations.”); Andrew Cunningham, *iPhone vs. Android: Which Is Better for You?*, N.Y. TIMES, May 16, 2023, <https://www.nytimes.com/wirecutter/reviews/ios-vs-android/> (stating that “great budget Android phones—including a few that will actually get prompt software updates—are available for \$200 or less”).

<sup>14</sup> REBECCA SKLOOT, *THE IMMORTAL LIFE OF HENRIETTA LACKS* 15 (2010).

<sup>15</sup> *Id.*

<sup>16</sup> Editorial, *Henrietta Lacks: Science Must Right a Historical Wrong*, NATURE, Sept. 1, 2020, <https://www.nature.com/articles/d41586-020-02494-z>.



### C. Unavoidable transactions

Even when a service or provider typically is avoidable, there are times when an individual cannot avoid a specific transaction under circumstances that otherwise compromise voluntariness and/or knowledge. For example, tech reporter Shoshana Wodinsky recently described how she once used a prescription health app in order to get discounts on medications she needed.<sup>17</sup> She was dismayed to learn later that the app had been sharing the names of her prescriptions with third parties.<sup>18</sup> She observed, “sometimes people don’t have a choice when they download an app or piece of tech. In my case, the drugs from this app were anti-depressants. If I couldn’t afford them, I would not have been functional.”<sup>19</sup>

A specific transaction could be unavoidable because the individual urgently needs something, and does not have the time or resources to seek out alternatives. For example, consider a situation in which an individual has a time-sensitive need to hop in a taxi and has no choice but to share information about their origin and destination locations (and perhaps additional information if they don’t carry cash and must pay by credit card) to get the ride. The sharing in that context is not an entirely volitional act because it is urgently needed. Further, the information sharing may be done without knowledge of the terms of the information sharing because the individual does not have time to inquire about or process the terms.

Anyone may sometimes face an unavoidable transaction, but people of limited means are bound to encounter such transactions with particular frequency because they are less likely to have the time or resources to find an alternative to an offered transaction. Consider, for example, a worker asked to submit to a pre-employment health screening or drug test, thereby sharing private medical information about themselves. A worker who cannot afford to turn down the job—who does not have the resources to forgo pay or seek employment elsewhere—may find this information sharing unavoidable. Indeed, research indicates that information about drug use is more likely to be demanded of low-income workers of color. A 2013 study by researchers at the Yale School of Medicine found that 63% of Black workers worked in a workplace that performed drug testing, compared to 46% of white workers, and 54% of non-white collar employees worked in a workplace that performed drug testing, compared to 44% of white collar employees.<sup>20</sup>

As another example, consider a situation in which a provider charges its customers different rates, with a lower rate for customers who agree to let it collect and use their personal information, and a higher rate for customers who exercise certain privacy-protective options. A customer with some disposable income may be able to pay the premium necessary to avoid sharing their personal information

---

<sup>17</sup> Charlie Warzel, *The Internet’s Original Sin*, GALAXY BRAIN (Sept. 23, 2021), <https://warzel.substack.com/p/the-internets-original-sin>.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* (internal quotation marks omitted).

<sup>20</sup> William C. Becker, Salimah Meghani, Jeanette M. Tetrault, & David A. Fiellin, *Racial/Ethnic Differences in Report of Drug Testing Practices at the Workplace Level in the U.S.*, 23 AM. J. ADDICTIONS 357, 359 (2014).

in a situation such as this, but one struggling to make ends meet may find the premium impossible to pay, and thus the information sharing unavoidable. This type of arrangement was offered a few years ago by a major internet service provider,<sup>21</sup> and defended by others, with one company arguing before the Federal Communications Commission that “a bargained-for exchange of information for service is a perfectly acceptable and widely used model throughout the U.S. economy.”<sup>22</sup> But as researchers at New America argued in 2019, “some pay-for-privacy regimes effectively coerce users—especially low-income consumers—into giving up their privacy if the discount is so disproportionate that users essentially have no choice.”<sup>23</sup>

#### D. Practical unavailability

Finally, even when information is sought from an individual in a context in which neither the service, provider, nor transaction is unavoidable, the information sharing may nevertheless be unavoidable as a practical matter due to a lack of knowledge on the part of the individual about the terms of the information sharing. Oftentimes, this could be due to a lack of transparency on the part of the information collector, but it could also be caused by confusion or overwhelm on the part of the individual compromising their ability to exercise an affirmative choice.

Lack of transparency may often render an otherwise avoidable information sharing unavoidable. Consider, for example, the case of Nomi Technologies, a company that tracked individuals as they moved around inside the stores of retailers that used its services.<sup>24</sup> Neither Nomi nor its clients informed individuals that the tracking was taking place.<sup>25</sup> As a result, even though undoubtedly many people who were tracked by Nomi did not have any real need to be in the stores where they were tracked, they were not able to avoid the tracking because they did not know about it.

Even when an entity is technically more forthcoming about its information practices, confusing language in or presentation of disclosures might impede individuals’ understanding of what is happening to such an extent that they lack sufficient knowledge to avoid the information sharing. Indeed, research indicates

<sup>21</sup> David Auerbach, *Privacy Is Becoming a Premium Service*, SLATE, Mar. 31, 2015, <https://slate.com/technology/2015/03/at-t-gigapower-the-company-wants-you-to-pay-it-not-to-sell-your-data.html>.

<sup>22</sup> Comcast Notice of Ex Parte, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (filed Aug. 1, 2016), *available at* <https://ecfsapi.fcc.gov/file/10802205606782/Comcast%20Ex%20Parte%20--%20WC%20Dkt%20No%2016-106%20--%207-28%20WCB%20Meeting.pdf>.

<sup>23</sup> BECKY CHAO & ERIC NULL, PAYING FOR OUR PRIVACY: WHAT ONLINE BUSINESS MODELS SHOULD BE OFF-LIMITS? 16 (2019), [https://d1y8sb8igg2f8e.cloudfront.net/documents/Paying\\_for\\_Our\\_Privacy\\_What\\_Online\\_Business\\_Models\\_Should\\_Be\\_Off-Limits\\_2019-0\\_0KCYFY4.pdf](https://d1y8sb8igg2f8e.cloudfront.net/documents/Paying_for_Our_Privacy_What_Online_Business_Models_Should_Be_Off-Limits_2019-0_0KCYFY4.pdf).

<sup>24</sup> FED. TRADE COMM’N, *Retail Tracking Firm Settles FTC Charges it Mised Consumers About Opt Out Choices* (Apr. 23, 2015), <https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-mised-consumers>.

<sup>25</sup> *Id.*

that many privacy policies do not effectively communicate what information will be collected and how it will be used.<sup>26</sup>

Practical unavailability, like other categories of unavailability, may confront different individuals differently depending on their circumstances. One might reasonably assume that challenges presented by lengthy, confusing privacy disclosures and confusing choices are more easily navigated by privileged individuals with the time and resources to be able to research, discover, and act on information not widely transparent to all. But research conducted by the Pew Research Center indicates that lower-income individuals are more likely to read privacy policies than those with higher incomes.<sup>27</sup> Similarly, a team of researchers led by Joseph Turow found that white and more educated respondents were more likely to express resignation vis-à-vis the state of online privacy compared with non-whites and respondents with a high school education or less.<sup>28</sup> On the other hand, when journalist Kevin Litman-Navarro evaluated privacy policies using the Lexile measure of readability, he found that the vast majority exceed the college reading level.<sup>29</sup> Citing statistics on American literacy levels, he concluded, “[A] significant chunk of the data collection economy is based on consenting to complicated documents that many Americans can’t understand.”<sup>30</sup>

### III. UNAVOIDABILITY AS AN EVER-PRESENT CONSIDERATION THROUGHOUT THE HISTORY OF U.S. PRIVACY LAW

Unavailability of information sharing has always been an important policy consideration in establishing privacy rules. Throughout the history of U.S. privacy law, as contexts emerged in which information sharing was unavoidable, policymakers recognized that change and responded by advancing policies to protect information shared in those contexts. As they advanced these policies, policymakers relied on the same few oft-repeated rationales to justify heightened protections for information shared unavoidably.

<sup>26</sup> See generally Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users’ Understanding*, 30 BERKELEY TECH. L. J. 39, 74-75 (2015).

<sup>27</sup> Brooke Auxier et al., *Americans’ Attitudes and Experiences with Privacy Policies and Laws*, PEW RSCH. CTR. (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/> (68% of adults in households with an annual income of \$30,000 or less say they ever read privacy policies, compared with 52% in households with an annual income of \$75,000 or more. People in lower income households are twice as likely to read all the way through as those in higher income households—30% vs. 15%).

<sup>28</sup> Joseph Turow, Michael Hennessy, & Nora Draper, *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*, U. OF PENN. ANNENBERG SCHOOL FOR COMMUNICATION 15 (2015), <https://core.ac.uk/download/pdf/30671899.pdf>.

<sup>29</sup> Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. TIMES, June 12, 2019, <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>.

<sup>30</sup> *Id.*

This is not to say that unavailability is or has been dispositive in determining what level of privacy protection to assign to information, because policymakers certainly have also considered other factors, including the norms and expectations of information subjects, the degree of sensitivity of information shared, and the severity of direct and tangible harms caused or likely to be caused by information sharing. But if policymakers have been relying upon variations of an unstated formula to determine the level of privacy protection appropriate for information shared under particular conditions, the unavailability of the information sharing has consistently been a key—though underappreciated—variable.

This Section explores the history of several areas of existing U.S. privacy law to examine whether and to what extent unavailability was an important factor for policymakers. These areas are explored in roughly chronological order: medical privacy, attorney-client privilege, communications privacy, financial privacy, Fourth Amendment third-party doctrine, educational privacy, and Section 5 of the FTC Act. In several of these areas of law, policymakers not only considered unavailability, but appear to have been motivated by the emergence of unavailability in a changing factual context.

#### A. *Unavailability in Medical Privacy*

Healthcare is an easy example of an unavoidable service. It is recognized as essential in numerous contexts. It is named as a right in both the Universal Declaration of Human Rights<sup>31</sup> and the International Covenant on Economic, Social and Cultural Rights.<sup>32</sup> In the U.S., recognition of medical care as essential underpins the creation and ongoing support of numerous federal programs and statutes, including Medicare, the Affordable Care Act, and the Emergency Medical Treatment and Active Labor Act.

Heightened privacy for medical information is among the oldest privacy frameworks. Today, medical information is widely understood to be “sensitive” and enjoys special status under a number of state and federal laws. In addition, the Health Information Portability and Accountability Act (HIPAA) Privacy Rule sets federal privacy standards for health information collected by healthcare providers, health plans, and healthcare clearinghouses.<sup>33</sup>

But medical confidentiality is an ancient professional tradition, which developed as the profession expanded as a way of ensuring that practitioners were viewed as trustworthy to deliver their needed service to patients, as well as to protect vulnerable patients from harms caused by indiscreet sharing of their private information.<sup>34</sup> Indeed, medical confidentiality was well established in medical

---

<sup>31</sup> G.A. Res. 217 (III) A, *supra* note 4, at Art. 25.

<sup>32</sup> International Covenant on Economic, Social and Cultural Rights art. 12, Dec. 16, 1966, 993 U.N.T.S. 3, 6 I.L.M. 360.

<sup>33</sup> See U.S. Dep’t of Health and Human Servs., Health Information Privacy: General Overview, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/general-overview/index.html>.

<sup>34</sup> See discussion *infra* notes 45–56 and accompanying text.

ethics and at common law long before HIPAA was passed in 1996. For example, when HIPAA was passed, the American Medical Association's Code of Medical Ethics already provided that "the physician should not reveal confidential communications or information without the express consent of the patients."<sup>35</sup>

To better understand the roots of medical confidentiality, it is necessary to look back across millennia, to various oaths that were required of physicians as their professional society formed and developed standards, even in centuries before the Common Era. Perhaps most famously, the Greek physician Hippocrates, born in the fourth century BCE, is said to have required his students to take an oath that contained a confidentiality requirement. Published versions of what today is known as the Hippocratic Oath are widely recognized not to have been authored by Hippocrates, and likely to constitute the contributions of several different parties.<sup>36</sup> As commonly formulated, the translated Hippocratic Oath contains the commitment, "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about."<sup>37</sup>

The oath attributed to Hippocrates likely derived from even more ancient precursors, which then persisted in a variety of forms after the time of Hippocrates.<sup>38</sup> Some scholars claim that long before Hippocrates was even born,

---

<sup>35</sup> AMA Code of Medical Ethics § 5.05 (1996-1997). It now also states, more broadly, "The information disclosed to a physician by a patient should be held in confidence." <https://journalofethics.ama-assn.org/article/ama-code-medical-ethics-opinion-confidentiality-patient-disclosure-and-circumstances-under-which-it/2012-06>.

<sup>36</sup> See, e.g., JOHN REDMAN COXE, *THE WRITINGS OF HIPPOCRATES AND GALEN: EPITOMISED FROM THE ORIGINAL LATIN TRANSLATIONS* 41–42 (1846) ("It is scarcely to be credited that Hippocrates was the author of this oath . . . . A strong presumption of its not being his, may be derived from the oath itself, in which every means of inducing abortion is sedulously prohibited; and yet, in the treatise 'De natura pueri,' we find a female made to abort under the author's exclusive direction and prescription."); *The Charters of Medical Ethics*, 1 BRITISH MED. J. 1262 (May 25, 1907) ("The authorship of the 'Hippocratic' oath is unknown."); W.H.S. JONES, *THE DOCTOR'S OATH: AN ESSAY IN THE HISTORY OF MEDICINE* 39 (1924) ("The document called 'the Hippocratic oath' presents many problems the answers to which seem to be lost for ever."); Helen King, *Hippocrates Didn't Write the Oath, So Why Is He the Father of Medicine?*, THE CONVERSATION, Oct. 2, 2014, <https://theconversation.com/hippocrates-didnt-write-the-oath-so-why-is-he-the-father-of-medicine-32334>; Hagop Kantarjian & David P. Steensma, *Relevance of the Hippocratic Oath in the 21st Century*, THE ASCO POST, Oct. 15, 2014 ("[T]he real original author of this most famous text in Western medicine is unknown, and there may have been several authors."); Owen Ress, *Did Hippocrates Write the Hippocratic Oath?*, BAD ANCIENT (June 8, 2020), <https://www.badancient.com/claims/hippocratic-oath/> ("we know from the work of the Roman medical writer Galen that even by his period, in the second century AD, people were questioning the authenticity of texts assigned to Hippocrates. . . . Really, we do not know of a single text that was written by Hippocrates.").

<sup>37</sup> Loren C. MacKinney, *Medical Ethics and Etiquette in the Early Middle Ages: The Persistence of Hippocratic Ideals*, 26 BULLETIN OF THE HISTORY OF MEDICINE 1, 31 (1952) (reprinting a translation from Ludwig Edelstein, *THE HIPPOCRATIC OATH* (1943)).

<sup>38</sup> A 1907 article in the British Medical Journal mentions theories that it may be derived from an "antique formula which had a priestly origin and in the course of time passed from the temple to the school," or that it may be of Egyptian origin, because "the Greeks who went to study medicine in Egypt had to submit there to ceremonies of initiation or investiture, which they

Indian physicians adhered to a similar oath that also contained a secrecy component.<sup>39</sup> In the early centuries CE, other oaths taken by medical practitioners contained similar commitments to secrecy (and shared many other similar features). Examples include the Charaka Samhita, a foundational Indian medical text edited by Maharishi Charaka around the first century CE,<sup>40</sup> and an oath for physicians that was described by the Ancient Hebrew physician Asaph in the sixth century CE.<sup>41</sup> Various oaths continued to proliferate and spread throughout medieval times in the Western world.<sup>42</sup>

Oaths derived from the ancient oaths continue to be administered to medical professionals today. In response to a 2009 survey of physicians in the U.S., 79% reported their medical school conducting an oath ceremony.<sup>43</sup> Most of those oaths include assurances of confidentiality.<sup>44</sup>

Although oaths containing a commitment to confidentiality seem to be ubiquitous in Western history, explicit discussions of the reasoning behind them are few and far between. As medical ethicist Ian E. Thompson observed in 1979, most of the available professional codes “assume that the value of confidentiality is self-evident, and do not seriously examine the grounds for maintaining

---

afterwards introduced in an appropriately altered form into their own country.” *The Charters of Medical Ethics*, *supra* note 36, at 1262.

<sup>39</sup> See Jacob Jay Lindenthal & Claudewell Sidney Thomas, *Confidentiality in Clinical Psychiatry*, 11 MED. & L. 119, 119 (1992). According to some accounts, physicians in Ancient India were bound by something called “Vaidya’s Oath” that dated back to the fifteenth century BCE. See Alfred Gellhorn, *Medical Ethics—So What’s the Story?*, 13 IN VITRO 588, 589 (1977) (“ethical codes were probably formulated as soon as man began to receive care for his ailments by whatever means; although the first written record of which I am aware is the Oath of the Hindu Physician prepared about 1500 B.C.”); JOSHUA A. PERPER & STEPHEN J. CINA, WHEN DOCTORS KILL: WHO, WHY, AND HOW 11 (2010); Charles Loomis Dana, *The Peaks of Medical History; An Outline of the Evolution of Medicine for the Use of Medical Students and Practitioners* 18 (1926) (supposed translation of this oath containing the line, “[w]hat happens in the house must not be mentioned outside.”).

<sup>40</sup> GERRIT J. MEULENBELD, A HISTORY OF INDIAN MEDICAL LITERATURE 114 (1999) (stating that Charaka “cannot have lived later than about A.D. 150-200 and not much earlier than about 100 B.C.”); *The Charters of Medical Ethics*, *supra* note 36, at 1262 (stating that M. Sylvain Lévi, Professor of Sanskrit at the Sorbonne, assigns Charaka “with confidence” to the first century); AVINASH C. KAVIRATNA, CHARAKA-SAMHITA (TRANSLATED INTO ENGLISH) 556 (1903) (translating this point in the text to “Thou shouldst never give out (to others) the practices of the patient’s house.”); PRIYADARANJAN RAY & HIRENDRA N. GUPTA, CARAKA SAMHITA (A SCIENTIFIC SYNOPSIS) 21 (1965) (“He must not divulge any information about the patient and his household.”).

<sup>41</sup> See Sussman Muntner, *Hebrew Medical Ethics and the Oath of Asaph*, 205 J. AMER. MED. ASSN. 912, 912–913 (1968) (translation: “do not divulge a man’s secret that he has confided unto you.”).

<sup>42</sup> JONES, *supra* note 36, at 41 (“The two versions of *Oath*, pagan and Christian, and the peculiar variants they present, particularly the variants of the Christian oath, suggest that the document had a wide circulation, and that the text was far from being stereotyped.”).

<sup>43</sup> Ryan M. Antiel, Farr A. Curlin, & Christopher Hook, *The Impact of Medical School Oaths and Other Professional Codes of Ethics: Results of a National Physician Survey*, 171 ARCH INTERN MED. 469, 470 (2011); (also finding that 97% participated in their medical school’s ceremony).

<sup>44</sup> See Howard Markel, “I Swear by Apollo”—On Taking the Hippocratic Oath, 350 N. ENGL. J. MED. 2026, 2028 (2005).

relationships of confidentiality, nor do they provide adequate moral or philosophical justification for doing so.”<sup>45</sup>

Looking at contextual clues accompanying ancient oaths, however, it appears likely that the prevailing rationale generally has been to promote trust in medical providers, on the reasoning that medical care is essential and therefore must be trustworthy. Jerome of Stridon (also known as “Saint Jerome”) drew a connection between the duty of confidentiality that fell on the physician and a similar duty falling on clergy. In a letter written in the 4th century, Jerome compared the Hippocratic oath to priests’ confidentiality obligation:

It is part of your [priests’] duty to visit the sick, to be acquainted with people’s households, with matrons, and with their children, and to be entrusted with the secrets of the great. Let it therefore be your duty to keep your tongue chaste as well as your eyes. Never discuss a woman’s looks, nor let one house know what is going on in another. Hippocrates, before he will instruct his pupils, makes them take an oath and compels them to swear obedience to him. That oath exacts from them silence, and prescribes for them their language, gait, dress, and manners.<sup>46</sup>

Many sources discuss a connection between confidentiality and physicians’ honor and reputation. For example, one common version of the ancient Hippocratic Oath states that it would be “shameful” to speak about things “seen or heard . . . in regard to the life of men,” and goes on to plead that if the oathtaker abides by the oath, “may it be granted to me to enjoy life and art, being honored with fame among all men for all time to come.”<sup>47</sup> A text seen in manuscripts from the tenth and fourteenth centuries describes the “sort of person a physician should be” and includes the passage, “Keep secret everything that goes on or is spoken in the home. Thus the physician himself, and the art, will acquire greater praise.”<sup>48</sup> A treatise that was popular from the ninth to the fifteenth century also counsels confidentiality,<sup>49</sup> and states at the end, “You will win more thanks if you do all these things, and no physician will be greater than you [in reputation].”<sup>50</sup> Another treatise from approximately 1100 CE states that students of medicine should have certain qualities and that teachers should “keep unworthy persons from entering this learned profession,” and advises that among other necessary qualities and

---

<sup>45</sup> Ian E. Thompson, *The Nature of Confidentiality*, 5 J. MED. ETHICS 57, 57 (1979).

<sup>46</sup> Letter from St. Jerome to Nepotian, in 1933 SELECT LETTERS OF ST. JEROME 189, 225 (F.A. Wright trans.).

<sup>47</sup> LUDWIG EDELSTEIN, *THE HIPPOCRATIC OATH* (1943), reprinted in Loren C. MacKinney, *Medical Ethics and Etiquette in the Early Middle Ages: The Persistence of Hippocratic Ideals*, 26 BULLETIN OF THE HISTORY OF MEDICINE 1, 31 (1952).

<sup>48</sup> *Id.* at 12.

<sup>49</sup> *Id.* at 23 (“Cherish modesty, follow chastity, guard the secrets of the homes [you visit]. If you know anything derogatory concerning a patient, keep quiet about it.”).

<sup>50</sup> *Id.* at 23–24.

behaviors, a physician “ought to keep to himself confidential information concerning the ailment.”<sup>51</sup>

There is, of course, an independent value to honor. But based on these examples, it is reasonable to conclude that the confidentiality mandated by various oaths serves the goal of elevating the reputation—thus engendering trust—of the profession itself.

In modern times, trust has frequently been raised as a reason to protect information shared in the unavoidable medical context. For example, in 1983, physician and reporter Lawrence K. Altman wrote in the *New York Times*,

From the time of Hippocrates, doctors have sworn to protect the confidentiality of the information given to them by patients in the belief that the privacy of the patient-doctor relationship is an integral part of the healing process. That confidentiality has been viewed as a bond of trust that allows patients to confide in physicians all sorts of intimate details that they otherwise might not reveal to anyone else.<sup>52</sup>

In 2000, when the Department of Health and Human Services (HHS) adopted the first HIPAA Privacy Rule, it also justified the rule as a way to engender trust in healthcare. HHS explained, “The clinician must trust the patient to give full and truthful information about their health, symptoms, and medical history. The patient must trust the clinician to use that information to improve his or her health and to respect the need to keep such information private.”<sup>53</sup>

The lack of voluntariness in much medical care has also been thought relevant to the protection of information shared with providers. For example, HHS recognized that “[t]he need for privacy of health information, in particular, has long been recognized as critical to the delivery of *needed* medical care.”<sup>54</sup> In one exploration of medical confidentiality, Ian Thompson described lack of voluntariness in the context of vulnerability:

The patient approaches the doctor under duress of fear, pain or need. This means that the patient is inherently vulnerable and disadvantaged in relation to the doctor. The ‘contract’ between them is not a contract as between equals (hence it may be misleading to speak as some sociologists do of patients as ‘consumers’). The patient is a patient (i.e. a sufferer), a person who may well be conforming to the sick role, but whose disease has forced him to

---

<sup>51</sup> *Id.* at 27.

<sup>52</sup> Lawrence K. Altman, *The Doctor’s World; Physician-Patient Confidentiality Slips Away*, N.Y. TIMES (Sept. 27, 1983), <http://www.nytimes.com/1983/09/27/science/the-doctor-s-world-physican-patient-confidentiality-slips-away.html>.

<sup>53</sup> Standard for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82467 (Dec. 28, 2000).

<sup>54</sup> *Id.* at 82467 (emphasis added); *see id.* At 82753 (“If people do not have confidence that their medical privacy will be protected, they will be much less likely to allow their records to be used for any purpose or might even avoid obtaining necessary medical care.”) (emphasis added).



accept the limitations and obligations of that role as well as its possible advantages.<sup>55</sup>

Writing about confidentiality in psychiatry, scholars Jacob Jay Lindenthal and Claudewell Sidney Thomas stated, “It has long been known that an individual presenting himself or herself to a physician for help in ameliorating symptoms casts the former, depending on the situation, in a relatively dependent, often frightening and vulnerable position.”<sup>56</sup> The discussion by Thompson, Lindenthal, and Thomas of patients being vulnerable, dependent, and forced to accept the terms of the relationship suggests an underlying theory that confidentiality must be upheld to protect the privacy rights of patients who cannot protect it for themselves.

### B. Unavoidability in Attorney-Client Privilege and Confidentiality

Heightened privacy protections have applied to information clients shared with their attorneys for centuries. For example, evidentiary privilege permits clients to shield from a court the information that they have shared with their attorney. A historical examination reveals that as the legal system became more complex and legal representation more widely recognized as essential, this triggered judges to establish the privilege in consideration of emerging unavoidability—the lack of voluntariness in a client’s sharing of information with their attorney.

Early discussions of attorney-client privilege at common law entail judges grappling with the fact that clients could no longer avoid sharing information with their attorneys. In the 1743 English case *Annesley v. Anglesea*, Baron Mounteney explained, “[A]n increase of legal business, and the inability of parties to transact that business themselves, made it *necessary* for them to employ . . . other persons who might transact that business for them.”<sup>57</sup> He further reasoned that because the relationship between attorneys and clients is one of necessity, the law must protect the information that flows between them in order to foster trust in the relationship: “[T]his necessity [for people to seek legal counsel] introduced with it the necessity of what the law hath very justly established, an inviolable secrecy to be observed by attorneys, in order to render it safe for clients to communicate to their attorneys all proper instruction for the carrying on those causes which they found themselves under a necessity of intrusting to their care.”<sup>58</sup> The necessity point was reiterated in later cases. In *Bramwell v. Lucas* (also in England) in 1824, the court held that “the ground upon which the privilege rests is, that it may be *necessary* for the protection of a man’s rights that he should make confidential communications to his attorney. That being the reason of the privilege, all communications collateral to the business of an attorney are of course excluded.”<sup>59</sup>

---

<sup>55</sup> Ian E. Thompson, *The Nature of Confidentiality*, 5 J. MED. ETHICS 57, 59 (1979).

<sup>56</sup> Jacob Jay Lindenthal & Claudewell Sidney Thomas, *Confidentiality in Clinical Psychiatry*, 11 MED. & L. 119, 119 (1992).

<sup>57</sup> *Annesley v. Anglesea*, 17 How. St. Trials 1139, 1241 (1743) (emphasis added).

<sup>58</sup> *Id.*

<sup>59</sup> *Bramwell v. Lucas*, 107 Eng. Rep. 560, 560–61 (1824) (emphasis added).

Because the attorney-client privilege was premised on the unavailability of the information sharing between a client and their attorney, courts did not extend the privilege to divulgences that were not necessary to the representation, and thus were more voluntary in nature. The Chief Baron presiding over *Annesley v. Anglesea* explained,

Nor do I see any impropriety in supposing the same person to be trusted in one case as an attorney or agent, and in another as a common acquaintance. In the first instance, the Court will not permit him, though willing, to discover what came to his knowledge as an attorney, because it would be in breach of that trust which the law supposes to be necessary between him and his employer: but where the client talks to him at large as a friend, and not in the way of his profession, I think the Court is not under the same obligations to guard such secrets, though in the breast of an attorney.<sup>60</sup>

The understanding of attorney-client privilege as protection for information shared unavoidably persisted beyond English common law, as courts in the New World grappled with related questions. For example, in the 1829 Vermont case *Dixon v. Parmelee*, the court stated,

It is the privilege of the client, that the mouth of his counsel should be forever sealed against the disclosure of things necessarily communicated to him for the better conducting his cause . . . but this privilege, in all the cases which have fallen under my observation, has been strictly confined to . . . where the substance of the communication was such that it became necessary for the attorney to know it in order to manage the suit.<sup>61</sup>

Not only are attorney-client relationships often necessary, but, as with physician-patient relationships, they flourish in a context of greater trust. In his landmark *Treatise on Anglo-American System of Evidence in Trials at Common Law*, John Henry Wigmore cited fostering trust as at the heart of evidentiary privileges. Wigmore asserted four conditions that generally must be met for evidentiary privilege to attach to communications between two persons (attorney and client, priest and penitent, or spouses). The named conditions included that “confidentiality must be essential to the full and satisfactory maintenance of the relation between the parties” and that the “relation must be one which in the opinion of the community ought to be sedulously fostered.”<sup>62</sup>

The unavailability of attorney-client communications is also recognized in support of lawyers’ professional obligation to hold such communications in

---

<sup>60</sup> *Id.* at 1239.

<sup>61</sup> *Dixon v. Parmelee*, 2 Vt. 185, 188 (1829).

<sup>62</sup> 5 JOHN HENRY WIGMORE, *TREATISE ON ANGLO-AMERICAN SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW* § 2285 (2d ed. 1923). The other two conditions named by Wigmore were that “[t]he communications must originate in a confidence that they will not be disclosed” and “[t]he injury that would inure to the relation by the disclosure of the communications must be greater than the benefit thereby gained for the correct disposal of litigation.” *Id.*

confidence. Trust continues to play a prominent role in discussions of attorneys' confidentiality duty. For example, in commentary accompanying the model rule on attorneys' duty of confidentiality, the American Bar Association observes, "The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct."<sup>63</sup> There, too, the trust rationale is named. The ABA explains that confidentiality "contributes to the trust that is the hallmark of the client-lawyer relationship."<sup>64</sup>

### C. *Unavoidability in Communications Privacy*

Interpersonal communications are essential. The Constitution included a Postal Clause for the purpose of facilitating communication, and several federal statutes have been established to promote the construction and management of communications networks. As new forms of communication have emerged and policymakers came to see those mediums as essential, additional privacy laws have been established.

The general inclination toward protecting the privacy of letters has been present since at least colonial times. Anuj Desai has argued that U.S. communications privacy "was intertwined with the early history of the post office."<sup>65</sup> According to Desai, surveillance of mail was a specific function of the British post office,<sup>66</sup> and that fact triggered several responsive policy developments in the colonies: the establishment of formal post offices in America,<sup>67</sup> promulgation of a regulation in the 1750s by deputy postmasters for the colonies requiring that all postmasters and associates subscribe to an oath that they would not tamper with the mail,<sup>68</sup> passage of a comprehensive postal ordinance in 1782 prohibiting postal officials from opening mail without a warrant,<sup>69</sup> and ultimately the inclusion of confidentiality in the first comprehensive postal statute in 1792.<sup>70</sup> By the time that statute was passed, the concept of correspondence privacy had been well established and there was no real debate.<sup>71</sup>

---

<sup>63</sup> American Bar Association, *Rule 1.6 Confidentiality of Information - Comment*, [https://www.americanbar.org/groups/professional\\_responsibility/publications/model\\_rules\\_of\\_professional\\_conduct/rule\\_1\\_6\\_confidentiality\\_of\\_information/comment\\_on\\_rule\\_1\\_6/](https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/).

<sup>64</sup> *Id.*

<sup>65</sup> Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 558 (2007); *id.* at 565 ("the principle of confidentiality of the mail in the American postal network dates back to, and is intimately intertwined with, the revolutionary goals of those who sought independence").

<sup>66</sup> *Id.* at 559–60; *id.* at 564 ("[B]y 1773, the Americans clearly worried, and had good reason to worry, that loyalist postmasters would intercept and read their letters, a frightening prospect when much of what they were doing likely constituted treason.").

<sup>67</sup> *Id.* at 562–63.

<sup>68</sup> *Id.* at 563.

<sup>69</sup> *Id.* at 565.

<sup>70</sup> *Id.* at 566.

<sup>71</sup> *Id.* at 567 ("It was, in short, well assumed by everyone that giving the government the power to intercept, open, and read correspondence was incompatible with the basic principles of a public communications network.").

When, in 1877, a Fourth Amendment challenge came before the Supreme Court in *Ex parte Jackson* regarding warrantless inspection of mail, the Court doubled down on the American tradition of correspondence privacy and ruled that letters and sealed packages sent through the mail were protected.<sup>72</sup> In doing so, the Court likened mailed papers to those “retained by the parties forwarding them in their own domiciles.”<sup>73</sup> The Court concluded that, “No law of Congress can place . . . any authority to invade the secrecy of letters . . . and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.”<sup>74</sup>

Decades later, telephones emerged on the scene, and soon were widely adopted as an easier means of facilitating communications. This forced courts and legislatures to step in to ensure that communications by phone receive strong privacy protection as well. Much of the legal activity on telephone privacy was precipitated by Prohibition-era wiretapping—Prohibition began in 1920, and telephones, which had become present in 35% of households by that time,<sup>75</sup> quickly became a favorite target of law enforcement agents seeking to ferret out bootleggers.<sup>76</sup> The policy response in defense of private communications was swift. By 1927, more than 25 states had made wiretapping a crime.<sup>77</sup>

Privacy protection of communications temporarily faltered, before being bolstered once again by legislators. In 1927, the Ninth Circuit Court of Appeals heard the appeal of a case against a Seattle bootlegger, Roy Olmstead, who contested the Fourth and Fifth Amendment constitutionality of evidence gained by federal agents through a telephone wiretap. By a 2 to 1 vote, the Court upheld Olmstead’s conviction, ruling that wiretapping did not violate the Constitution. But Judge Rudkin dissented, referencing *Ex Parte Jackson* and asking, “What is the distinction between a message sent by letter and a message sent by telegraph or by telephone?”<sup>78</sup> As he went on, Judge Rudkin appeared to consider the unavoidable nature of telephone communications and the unavoidability of wiretapping relevant, demanding,

Must the millions of people who use the telephone every day for lawful purposes have their messages interrupted and intercepted in this way? Must their personal, private, and confidential communications to family, friends, and business associates pass through any such scrutiny on the part of agents, in whose selection

---

<sup>72</sup> *Ex parte Jackson*, 96 U.S. 727 (1877).

<sup>73</sup> *Id.* at 733.

<sup>74</sup> *Id.*

<sup>75</sup> U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES: 1999, at 885 (1999).

<sup>76</sup> April White, *A Brief History of Surveillance in America*, SMITHSONIAN MAG. (Apr. 2018), <https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/>.

<sup>77</sup> PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 111 (1995).

<sup>78</sup> *Olmstead v. United States*, 19 F.2d 842, 850 (9th Cir. 1927), *aff’d*, 277 U.S. 438 (1928) (Rudkin, J., dissenting).

they have no choice, and for the faithful performance of whose duties they have no security?<sup>79</sup>

The following year, the case came before the Supreme Court, which upheld the Ninth Circuit's ruling but seemed troubled by this outcome. The majority almost explicitly called on Congress to correct it. Writing for the Court, Taft noted, "Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation."<sup>80</sup> In his concurrence, Justice Holmes called wiretapping "dirty business."<sup>81</sup>

After *Olmstead*, states continued to pass laws establishing protections for communications. By 1932, 26 states had enacted statutes making it a criminal offense to listen in on or tap wires, and 35 states plus Alaska prohibited a telegraph or telephone company from disclosing or assisting in the disclosure of any message.<sup>82</sup>

The federal Congress hotly debated the use of wiretapping as a Prohibition enforcement tool and the need for a federal wiretap law. Several members urged approval of an amendment, introduced by Rep. Tinkham of Massachusetts, prohibiting the expenditure of Prohibition enforcement funds for the purpose of tapping telephone and telegraph wires. Discussing the then-recent decision in *Olmstead*, Representative Beck raised the essential and unavoidable nature of interpersonal communications, referring to wiretapping as an "indefensible violation of the ordinary decencies of private life," describing the ability of an agent "to listen to everything you may say, messages of love and affection and of sacred confidence, or of the most intimate, confidential business."<sup>83</sup> In the Communications Act of 1934, Congress finally established federal wiretap protections.<sup>84</sup>

In large part because of this provision in the 1934 Act, the Federal Communications Commission has also considered communications deserving of particular privacy protection. By 1966, in the context of the first of the Computer Inquiries, the agency asserted, "Privacy, particularly in the area of communications, is a well-established policy and objective of the Communications Act. Thus, any

---

<sup>79</sup> *Id.*

<sup>80</sup> *Olmstead v. United States*, 277 U.S. 438, 465, 48 S. Ct. 564, 568, 72 L. Ed. 944 (1928), overruled in part by *Berger v. State of N.Y.*, 388 U.S. 41, 87 S. Ct. 1873, 18 L. Ed. 2d 1040 (1967), and overruled in part by *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967). Taft's invitation was heard—and later cited—by Congress. Cong. Rec. House 2902 (Jan. 22, 1931) (Rep. Beck, stating, "it is quite obvious, if you will read Chief Justice Taft's opinion, that he almost invited the action of this body to prevent" wiretapping).

<sup>81</sup> *Id.* at 470.

<sup>82</sup> Basil W. Kacedan, *The Right of Privacy*, 12 B.U. L. REV. 353, 382 (1932).

<sup>83</sup> CONG. REC. H2902 (Jan. 22, 1931).

<sup>84</sup> Communications Act of 1934 § 705, Pub. Law 73-416, 1064, 1103-1104 (June 19, 1934).

threatened or potential invasion of privacy is cause for concern by the Commission and the industry.”<sup>85</sup>

And although in *Olmstead* the Supreme Court—with regrets—declined to extend Fourth Amendment protection to a private phone conversation, in 1967 the Court overturned that decision in *Katz*. The Court seemed influenced in part by the essential and unavoidable nature of information sharing via public telephone. As it rejected the *Olmstead* framework, the Court stated, “To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”<sup>86</sup>

In recent years, as well, policymakers have continued to extend heightened privacy protections to essential communications services. In 1996, as part of the Telecommunications Act, Congress established a telecommunications privacy provision enshrining existing FCC policy in statute and generally prohibiting telecommunications carriers from using or sharing information about their customers’ use of the service for purposes other than as necessary to provide the service “[e]xcept as required by law or with the approval of the customer.”<sup>87</sup> When, in 2016, the Federal Communications Commission promulgated rules establishing strong privacy protections for information shared by customers with their broadband providers (these rules were later eliminated by Congress under a Congressional Review Act resolution), the agency observed that broadband was “essential for business growth and innovation,” and stated, “The privacy framework we adopt today will bolster consumer trust in the broadband ecosystem.”<sup>88</sup>

#### D. Unavoidability in Financial Privacy

Banking and credit are unavoidable in the modern economy. Financial privacy in the United States is protected by a variety of federal and state laws. An exploration of the history of financial privacy in the U.S. reveals that as burgeoning interest in law enforcement access to bank records grew in the 20th century, lawmakers responded by explicitly recognizing that formalized banking had become an essential service in the modern era, and that legislation was necessary to preserve individuals’ right to protect the privacy of the information they unavoidably shared with these providers.<sup>89</sup> This was the context in which U.S. lawmakers established legal protections for financial privacy.

---

<sup>85</sup> *In re Regul. & Pol’y Probs. Presented by the Interdependence of Computer & Comm’n Servs. & Facilities*, 7 F.C.C.2d 11, 16 (1966).

<sup>86</sup> *Katz v. United States*, 389 U.S. 347, 352 (1967) (“One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.”).

<sup>87</sup> 47 U.S.C. § 222(c)(1); *see* H.R. Rep. No. 104-204 (1995) (explaining the analogous provision in the House bill: “All carriers are prohibited from using the information for any service other than the service from which it is derived or if it is necessary in the provision of customer premise equipment. These new privacy rules will apply to all telecommunications carriers.”).

<sup>88</sup> FED. TRADE COMM’N, *Report and Order*, ¶ 37 (Nov. 2, 2016) <https://docs.fcc.gov/public/attachments/FCC-16-148A1.pdf>.

<sup>89</sup> *See* discussion *infra* notes 111–119 and accompanying text.

Prior to the passage of the first federal law concerning bank records, banks were guided by common law to protect the confidentiality of their customers' records.<sup>90</sup> In 1923, the English Court of Appeal issued a landmark opinion in *Tournier v. National Provincial and Union Bank of England* finding that bankers had an implied contractual obligation to:

not divulge to third persons, without the consent of the customer express or implied, either the state of the customer's account, or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, unless the banker is compelled to do so by order of a Court, or the circumstances give rise to a public duty of disclosure, or the protection of the banker's own interests require it.<sup>91</sup>

The *Tournier* court did not directly mention the unavailability of financial services, but did allude to it, and to the importance of fostering trust in the field. Comparing the banker's duty of confidentiality to similar duties adhered to by counsel, solicitors, and doctors, Lord Justice Bankes said in his written judgment, "[T]he underlying principle may be the same. The case of the banker and his customer appears to be one in which the confidential relationship . . . is very marked. The credit of the customer depends very largely upon the strict observance of that confidence."<sup>92</sup> Lord Justice Atkin relied on past judgments in stating that a court ought only to imply a contractual term when it is "such a necessary term that both parties must have intended that it should be a term of the contract, and have only not expressed it because its necessity was so obvious that it was taken for granted."<sup>93</sup> He continued, "Is there any term as to secrecy to be implied from the relation of banker and customer? I have myself no doubt that there is."<sup>94</sup>

A few years later in 1926, when Thomas B. Paton, general counsel of the American Bankers Association, released the first version of his digest of legal opinions, statutes, and decisions affecting the banking business, U.S. law was developing on the issue. Paton observed that where bankers had been called as witnesses in lawsuits against their customers, no evidentiary privilege had been found to permit the refusal of testimony, but that "as a general proposition . . . the

---

<sup>90</sup> *Foreign Bank Secrecy and Bank Records: Hearing on H.R. 15073 Before the H. Comm. on Banking and Currency*, 91st Cong. 317 (1970) (statement of Carl W. Desch, Senior Vice President, First National City Bank of New York, on Behalf of the New York Clearing House Association; accompanied by Roy C. Haberkern, Jr., Milbank Tweed, Hadley & McCloy; and Henry Harfield, Shearman & Sterling) ("In this country, banks as a matter of common law are liable to their customers for damages if they, without consent or proper legal compulsion, disclose to anyone . . . information as to the affairs of such customers."); see Mary Catherine Green, *The Bank Secrecy Act and the Common Law: In Search of Financial Privacy*, 7 ARIZ. J. INT'L & COMP. L. 261, 262-63 (1989); Nancy M. Kirschner, *The Right to Financial Privacy Act of 1978—The Congressional Response to United States v. Miller: A Procedural Right to Challenge Government Access to Financial Records*, 13 U. MICH. J. L. REFORM 10, 14 (1979).

<sup>91</sup> *Tournier v. National Provincial and Union Bank of England*, 1 KB 461, 461 (1924).

<sup>92</sup> *Id.* at 474.

<sup>93</sup> *Id.* at 483.

<sup>94</sup> *Id.*

banker owes the customer a duty to keep the affairs of the latter confidential and not voluntarily disclose them to others, except under legal compulsion.”<sup>95</sup> At the time, however, Paton was “not aware of any reported case wherein damages have been sought or awarded for a breach of duty of this nature.”<sup>96</sup> Paton reported the then-recent decision in *Tournier*, noting that it was the first decision in England holding that a banker owed a depositor a legal duty of secrecy, not observing that English authorities had “for some time . . . inclined toward the recognition of such an obligation, although the cases which raised the question did not decide whether this duty is legal or merely moral.”<sup>97</sup>

Financial confidentiality may not have been well established in 1926, but over the ensuing decades, U.S. courts agreed with the *Tournier* court’s finding that banks owed a duty of confidentiality to their customers. For example, a few years later, in 1929, a New Jersey court denied a prosecutor the right to inspect records of accounts of all the police of Newark, New Jersey, without opening a grand jury investigation and issuing subpoenas. The judge reasoned, “There is an implied obligation, as I see it, on the bank, to keep these from scrutiny until compelled by a court of competent jurisdiction to do otherwise.”<sup>98</sup> Forty years later, when a Florida court also permitted a complaint for breach of a bank’s implied contractual duty of confidentiality, the court observed, “From the leading cases, a qualified duty of non-disclosure appears to be evolving in both England and America.”<sup>99</sup> By that time the implied duty was widely recognized enough to be included in summaries of U.S. law. The Florida court quoted *American Jurisprudence* as stating, at the time “it is an implied term of the contract between a banker and his customer that the banker will not divulge to third persons, without the consent of the customer, express or implied, either the state of the customer’s account or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, unless the banker is compelled to do so by order of a court . . . .”<sup>100</sup>

The implied duty became more ossified over the years. In 1961, when a bank in Idaho disclosed a depositor’s financial condition to his employer, the Supreme Court of Idaho allowed a claim based on breach of an implied contract that the bank would not disclose information concerning an account to third persons without authorization. In strong words, the court declared it “inconceivable that a bank would at any time consider itself at liberty to disclose the intimate details of its depositors’ accounts,” asserting, “Inviolable secrecy is one of the inherent and

---

<sup>95</sup> THOMAS B. PATON, PATON’S DIGEST 1199 (1926).

<sup>96</sup> *Id.*

<sup>97</sup> *Id.* (citing *Hardy v. Veasey*, L. R. 3 Ex. 107; *Foster v. Bank of London*, 3 F. & F. 14).

<sup>98</sup> *Brex v. Smith*, 104 N.J. Eq. 386, 390, 146 A. 34, 36 (Ch. 1929).

<sup>99</sup> *Milohnich v. First Nat. Bank of Miami Springs*, 224 So. 2d 759, 761 (Fla. Dist. Ct. App. 1969). *Cf.* *Barnett Bank of W. Fla. v. Hooper*, 498 So. 2d 923 (Fla. 1986).

<sup>100</sup> *Id.* (quoting 10 FRANCIS C. AMENDOLA ET AL., *AMERICAN JURISPRUDENCE, BANKS AND FINANCIAL INSTITUTIONS* § 332 (2d ed. 2023)).



fundamental precepts of the relationship of the bank and its customers or depositors.”<sup>101</sup>

Although bankers’ implied duty of confidentiality gradually became better established over the decades, no federal statutes addressed the privacy of financial records until 1970, when the Bank Secrecy Act and the Fair Credit Reporting Act were both passed as part of the same package of updates to the Federal Deposit Insurance Act.<sup>102</sup> The purpose of the Fair Credit Reporting Act (FCRA) was to “ensure the confidentiality, accuracy and relevancy of information reported on consumers.”<sup>103</sup> The Bank Secrecy Act, on the other hand, was in fact passed not to strengthen privacy protections for financial records, but to facilitate the maintenance of and law enforcement access to such records for the purpose of fighting money laundering and white collar crimes.<sup>104</sup> Because it was a law designed to force disclosure, rather than to foster secrecy, as the title might have indicated, then—House Representative Ed Koch of New York opined in 1975 that it “might very well be the most misnamed piece of legislation ever enacted.”<sup>105</sup>

The Bank Secrecy Act was disliked by many and in the early 1970s bankers, bank customers, and the ACLU challenged it on a variety of grounds, including the Fourth Amendment, but the Supreme Court, in a six-three decision, upheld the law and its implementing regulations in 1974.<sup>106</sup> Later that year, as discussed below in the discussion of third-party doctrine, the California Supreme Court found in *Burrows v. Superior Court* that a bank customer had a reasonable expectation of privacy—as protected by the analog to the Fourth Amendment in the California Constitution—in copies of statements from a bank in which they maintained an

---

<sup>101</sup> *Peterson v. Idaho First Nat. Bank*, 83 Idaho 578, 588, 367 P.2d 284, 290 (1961). Even courts that did not find financial records protected by law recognized banks’ general obligation to safeguard the privacy of their customers. For example, in 1946, a federal judge in Alabama found that a taxpayer was not protected by the Fourth Amendment from inspection by an Internal Revenue Commissioner of bank-held financial records but acknowledged that such records generally ought to be held in confidence by the institution. In his opinion he proclaimed, “[a]ll agree that a bank should protect its business records from the prying eyes of the public, moved by curiosity or malice. No one questions its right to protect its fiduciary relationship with its customers, which, in sound banking practice, as a matter of common knowledge, is done everywhere.” *United States v. First Nat. Bank of Mobile*, 67 F. Supp. 616, 624 (S.D. Ala. 1946).

<sup>102</sup> Federal Deposit Insurance Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114.

<sup>103</sup> *Id.* at 1128. (“It is the purpose of this title to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this title.”).

<sup>104</sup> *Id.* at 1116. (“It is the purpose of this chapter to require the maintenance of appropriate types of records and the making of appropriate reports by such businesses in the United States where such records or reports have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.”).

<sup>105</sup> Federal Deposit Insurance Act of 1970, Hearings on H.R. 8024 Before the Subcomm. on Financial Institutions Supervision, Regulation and Insurance of the H. Comm. On Banking, Currency, and Housing. 94<sup>th</sup> Cong. 527 (1975) (statement of Hon. Edward I. Koch, a representative in Congress from the state of New York).

<sup>106</sup> *California Bankers Ass’n v. Shultz*, 416 U.S. 21, 94 S. Ct. 1494, 39 L. Ed. 2d 812 (1974).

account.<sup>107</sup> The California court found it quite relevant that banking is an essential service and that sharing information with a bank is unavoidable—that it lacks voluntariness—explaining, “For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account.”<sup>108</sup>

When a similar controversy came before the U.S. Supreme Court a couple years later in *Miller*, the Court departed from California and found that a Fourth Amendment reasonable expectation of privacy did *not* extend to records held by a bank, due to third-party doctrine.<sup>109</sup> The majority was not persuaded of the customer’s Fourth Amendment interest in records held by their bank, but Justice Brennan dissented, quoting at length from *Burrows*, because he agreed with California that the sharing of information with a bank lacks voluntariness.<sup>110</sup>

The *Miller* decision was surprising and concerning to a number of bankers, customers, and policymakers, and sparked an interest in new legislation that would affirmatively establish privacy protections for bank records. For example, in congressional hearings, then-Representative Barry Goldwater of California argued, “[G]iven the startling and unacceptable legal contentions contained in the Supreme Court decision of June of last year, *United States v. Miller*, Federal legislation is required.”<sup>111</sup> Representative Edward Pattison of New York said, “The banking industry has tried to impose some restraints on access to customers’ records, but last year’s decision in the *Miller* case destroyed their last line of defense.”<sup>112</sup> In testimony before a House subcommittee, John Rolph of the American Bankers Association stated, “[T]he *Miller* case put the lid on the concept of there being any claim of confidentiality under the fourth amendment for bank customer records,” and speaking in support of the Safe Banking Act of 1977, said, “This bill [and others] . . . clearly tend to turn this result around. Congress has the power to enact legislation to reverse the effect of recent interpretations of the Supreme Court.”<sup>113</sup>

---

<sup>107</sup> *Burrows v. Superior Ct.*, 13 Cal. 3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1974); *see* discussion *infra* notes 2-3 and accompanying text.

<sup>108</sup> *Id.* at 247.

<sup>109</sup> *United States v. Miller*, 425 U.S. 435 (1976).

<sup>110</sup> *Id.* at 447.

<sup>111</sup> Safe Banking Act of 1977, Hearings on H.R. 9086 Before the Subcomm. on Financial Institutions Supervision, Regulation and Insurance of the H. Comm. On Banking, Financial and Urban Affairs. 95<sup>th</sup> Cong. 1458 (statement of Hon. Barry M. Goldwater, Jr., a representative in Congress from the state of California). Goldwater also served on the Privacy Protection Study Commission that released an influential final report in 1977. *Id.* at 1459 (“My recommendations for modification are based on several years of detailed study and investigations of personal informational privacy and my activities over the past 2 years on the Privacy Protection Study Commission.”)

<sup>112</sup> *Id.* at 1469. (statement of Hon. Edward W. Pattison, a representative in Congress from the state of New York).

<sup>113</sup> *Id.* at 1600. (statement of Mr. John F. Rolph, tax counsel of the American Bankers Association).

Calls for federal legislation to improve the state of financial privacy grew, as policymakers recognized that the growth of the credit industry and electronic records made the sharing of financial information more unavoidable than ever for individuals. During that time, a Privacy Protection Study Commission created by the Privacy Act of 1974 was developing a report on *Personal Privacy in an Information Society*. In the report it finally issued in 1977, the Commission acknowledged, “Credit is essential for the vast majority of Americans.”<sup>114</sup> Echoing the language of the *Burrows* court, the Commission said about “organizations that depend on the accumulation of extremely detailed records about the individual’s activities, such as those compiled by a bank,” that “while in theory these relationships are voluntary, in reality an individual today has little choice but to establish them as he would be severely, and perhaps insurmountably, disadvantaged if he did not.”<sup>115</sup>

The Commission’s report was interpreted in Congress as supportive of efforts to pass financial privacy legislation, and its conclusions and recommendations were echoed by legislators.<sup>116</sup> For example, Representative Cavanaugh stated, “It was pointed out by the Privacy Protection Study Commission in their final report, entitled ‘Personal Privacy in an Information Society,’ that financial records . . . provide another instance where the changing patterns of life took the possession of information about himself out of the control of the individual.”<sup>117</sup>

The following year, Congress passed the Right to Financial Privacy Act, the first federal statute that affirmatively established the confidentiality of records held by financial institutions.<sup>118</sup> A House report on the legislation explained, “The title is a congressional response to the Supreme Court decision in . . . *United States v. Miller*.”<sup>119</sup>

#### *E. Unavoidability in Fourth Amendment Third-Party Doctrine*

Unavoidability has also been a central consideration in determining when information shared by an individual with a third party receives Fourth Amendment

---

<sup>114</sup> Privacy Protection Study Commission, *PERSONAL PRIVACY IN AN INFORMATION SOCIETY* 41 (1977).

<sup>115</sup> *Id.* at 20.

<sup>116</sup> Safe Banking Act of 1977, Hearings on H.R. 9086 Before the Subcomm. on Financial Institutions Supervision, Regulation and Insurance of the H. Comm. On Banking, Financial and Urban Affairs. 95<sup>th</sup> Cong. 1458 (remarks of Representative Fernand J. St Germain, chairman) (stating that “[t]he recommendations of the Commission, in essence, confirm the judgment of the sponsors of” some of the privacy bills under consideration); *id.* at 1452 (remarks of Rep. Cavanaugh, quoting letter from Rep. Charles W. Whalen, Jr.) (“the report is out now . . . and it eliminates the last legitimate cause for delay in enacting Federal legislation to safeguard the privacy of third-party records.”)

<sup>117</sup> *Id.* at 1451. (remarks of Hon. John J. Cavanaugh, a representative in Congress from the state of Nebraska).

<sup>118</sup> Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641, 3697.

<sup>119</sup> H.R. Rep. No. 95-1383, at 34 (1978).

protection.<sup>120</sup> An examination of third-party doctrine cases over the years reveals that courts find both a lack of voluntariness and a lack of knowledge on the part of the information subject to be relevant in deciding whether to apply the third-party doctrine to the information at issue. Where courts have concluded that information sharing with a third party was unavoidable, judges have tended to also assert that that information should be protected as a matter of right—especially, and famously, in the recent *Carpenter* case involving cell phone location data.<sup>121</sup>

Before the third-party doctrine was developed, there were secret agent cases—cases in which courts considered the admissibility of information gathered secretly by someone wearing a wire. Both voluntariness and knowledge were discussed in this context. For example, in 1963, when the Supreme Court decided *Lopez v. United States*, it held that information the petitioner had shared with an undercover agent did not receive Fourth Amendment protection because the agent “was there with petitioner’s assent.”<sup>122</sup> In other words, the information subject acted voluntarily. The Court also contemplated the information subject’s knowledge, reasoning, “We think the risk that petitioner took in offering a bribe to Davis fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording.”<sup>123</sup> In other words, the petitioner knew or should have known that reproduction of his statements was a possible outcome of his conduct.

Acknowledgement and weighing of unavoidability are at the heart of the dissents as well as of the majority opinions in key third-party doctrine cases—especially in those involving records generated in the context of unavoidable services. Thirteen years after *Lopez*—and after the Court established the reasonable expectation of privacy test in *Katz*—when the Court decided *U.S. v. Miller*, it determined that checks and deposit slips could be obtained by law enforcement without a warrant because the respondent had had the opportunity to avoid sharing the information in question with a third party. Again, the Court cited voluntariness, stating, “All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”<sup>124</sup>

A few years before *Miller*, however, the California Supreme Court reached the opposite conclusion under its own Constitution. The California Supreme Court

---

<sup>120</sup> This observation is related to Orin Kerr’s previous argument that “third-party doctrine is better understood as a form of consent rather than as an application of *Katz*. Third-party disclosure eliminates privacy because the target voluntarily consents to the disclosure.” Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588 (2009).

<sup>121</sup> See discussion *infra* notes 124–130 and accompanying text.

<sup>122</sup> *Lopez v. U.S.*, 373 U.S. 427, 439 (1963).

<sup>123</sup> *Id.* at 439.

<sup>124</sup> *U.S. v. Miller*, 425 U.S. 435, 442 (1976). The Court had previously held that provisions of the Bank Secrecy Act of 1970 requiring banks to keep certain records of their customers’ financial transactions did not violate the Fourth Amendment, “the mere maintenance by the bank of records without any requirement that they be disclosed to the Government (which can secure access only by existing legal process) constituting no illegal search and seizure.” *California Bankers Ass’n v. Shultz*, 416 U.S. 21, 23, 94 S. Ct. 1494, 1498–99, 39 L. Ed. 2d 812 (1974).

found that because banking is an essential service, customers who share information with their financial institutions do not do so voluntarily. Considering facts similar to those at issue in *Miller*, the California court in *Burrows v. San Bernardino* observed that interacting with one's bank was "not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."<sup>125</sup> Justice Brennan shared the view of the California court, and when *Miller* came before the Supreme Court, he dissented from the application of third-party doctrine to the information at issue, explaining, "I dissent because in my view the California Supreme Court correctly interpreted the relevant constitutional language."<sup>126</sup>

Shortly after deciding *Miller*, the Court considered another third-party doctrine case involving an essential service—phone service—in *Smith v. Maryland*, and again declined to extend Fourth Amendment protection to the information in question based on the reasoning that the petitioner already voluntarily shared the information with third parties, thus assuming the risk. The court explained, "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."<sup>127</sup>

Justice Marshall famously dissented in *Smith v. Maryland*, joined by Justice Brennan, with the lack of voluntariness at the center of his dissent. Marshall did not quarrel with the premise, advanced by the majority, that information shared voluntarily with a third party ought not receive the same level of protection as unshared information. But he disagreed with the majority's determination that a person who placed phone calls voluntarily shared information about their phone communications with a third party, citing the fact that phones had become unavoidable. Marshall argued, "[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." Marshall was troubled by the fact that phones had become essential, and that therefore the sharing of information about one's phone habits was unavoidable.

Decades later, the Supreme Court in *Carpenter v. U.S.* declined to extend third-party doctrine to cell site location information in large part on the acknowledgment that cellular service had become an unavoidable service, undermining voluntariness in an individual's sharing of location information with their mobile service provider. The Court explained, "[w]e have previously held that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'"<sup>128</sup> But in this case,

---

<sup>125</sup> *Burrows v. Superior Court*, 13 Cal. 3d 238, 247 (1974).

<sup>126</sup> *U.S. v. Miller*, 425 U.S. 435, 447 (1976) (Brennan, J., dissenting).

<sup>127</sup> *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

<sup>128</sup> *Carpenter v. United States*, 138 S. Ct. 2206, 2216, 201 L. Ed. 2d 507 (2018) (quoting *Smith*, 442

the second rationale underlying the third-party doctrine—voluntary exposure—[does not] hold up when it comes to CSLI. Cell phone location information is not truly “shared” as one normally understands the term. In the first place, cell phones and the services they provide are “such a pervasive and insistent part of daily life” that carrying one is indispensable to participation in modern society. . . . Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily “assume[] the risk” of turning over a comprehensive dossier of his physical movements.<sup>129</sup>

Explaining and discussing the new multi-factor test applied by the Court in *Carpenter*, Paul Ohm has written, “[s]ome forms of data collection are inescapable because they relate to services one needs to use to be a functioning member of today’s society.”<sup>130</sup>

#### F. Unavoidability in Educational Privacy

Education is another essential service in the context of which information sharing is unavoidable. All 50 states and the District of Columbia have compulsory attendance laws that require children to attend school at least from the age of 7 to the age of 16.<sup>131</sup> The majority of states had compulsory attendance laws by 1890.<sup>132</sup> As information was collected from children in schools for various purposes, lawmakers expressed indignation at parents’ inability to avoid this information sharing and to defend the privacy of intimate family information, and stepped in to restore privacy as a matter of right.<sup>133</sup>

The law generally thought of as the nation’s federal education privacy statute was passed precisely to rein in unavoidable information flows taking place in schools. The Family Educational Rights and Privacy Act (FERPA) is perhaps best understood today for what it does—placing restrictions on, and providing certain access rights to, children’s education records.<sup>134</sup> But the legislative history indicates that FERPA was passed as a check on the administration of questionnaires and other evaluations on schoolchildren without their parents’ knowledge or permission, often involving the collection of intimate information about the children’s lives and

---

U. S., at 743–744).

<sup>129</sup> *Id.* at 2220 (quoting *Riley v. California*, 573 U.S. 373, 385 (2014); *Smith*, 442 U.S. at 745).

<sup>130</sup> Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J. L. & TECH. 357, 376 (2019).

<sup>131</sup> State Education Practices: Table 5.1. Compulsory school attendance laws, minimum and maximum age limits for required free education, by state: 2017, National Center for Education Statistics, [https://nces.ed.gov/programs/statereform/tab5\\_1.asp](https://nces.ed.gov/programs/statereform/tab5_1.asp) (last visited July 26, 2021).

<sup>132</sup> Michael S. Katz, *A HISTORY OF COMPULSORY EDUCATION LAWS* 17 (1976).

<sup>133</sup> See discussion *infra* notes 142–148 and accompanying text.

<sup>134</sup> See U.S. Department of Education, Family Educational Rights and Privacy Act (FERPA) <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html> (last visited July 26, 2021).

families. Parents and policymakers were outraged by the fact that children were compelled to disclose this information in the unavoidable context of mandatory education.

The primary sponsor of FERPA, Senator James Buckley, hailed from New York, a state that has had compulsory school attendance for children since the 1870s.<sup>135</sup> In the years before Senator Buckley introduced the legislation, controversies were bubbling up concerning schools' collection and maintenance of student records—and whether parents had the right to control or access those records.<sup>136</sup> In 1961, in a case called *Van Allen v. McCleary*, a New York court considered it relevant that attendance was compulsory when it granted a parent's mandamus petition to compel the production of his child's school records, after faculty at the school informed the parent that the child was in need of psychological treatment and therapy. Holding that the parent had a common law right to inspect the records, future Supreme Court Justice Brennan explained, "Petitioner's rights, if any, stem . . . from his relationship with the school authorities as a parent who under compulsory education has delegated to them the educational authority over his child."<sup>137</sup>

Senator Buckley was particularly inspired by a 1973 case called *Merriken v. Cressman* in the Eastern District of Pennsylvania—a case the senator explicitly referenced when he introduced the legislation that would become FERPA.<sup>138</sup> In *Merriken*, a child and parent challenged a school district program that used a detailed questionnaire in an attempt to identify potential drug abusers and prepare necessary interventions. The court described the invasive nature of the inquiry:

The questionnaires ask such personal and private questions as the family religion, the race or skin color of the student (Defendants have since stipulated to dropping this question), the family composition, including the reason for the absence of one or both parents, and whether one or both parents "hugged and kissed me good night when I was small", "tell me how much they love me", "enjoyed talking about current events with me", and "make me feel unloved". In addition both students and teachers are asked to identify other students in the class who make unusual or odd remarks, get into fights or quarrels with other students, make unusual or inappropriate responses during normal school activities, or have to be coaxed or forced to work with other pupils.<sup>139</sup>

---

<sup>135</sup> James D. Folts, History of the University of the State of New York and the State Education Department 1784 - 1996 (1996), available at <https://eric.ed.gov/?id=ED413839>.

<sup>136</sup> See National Committee for Citizens in Education, CHILDREN, PARENTS AND SCHOOL RECORDS (1974).

<sup>137</sup> *Van Allen v. McCleary*, 27 Misc. 2d 81, 91, 211 N.Y.S.2d 501, 512 (Sup. Ct. 1961).

<sup>138</sup> Senator Buckley referenced this case when he introduced the language that would become FERPA. 120 Cong. Rec. Senate 14,581 (May 14, 1974) (stating, "[t]his case is a microcosm of the problems addressed by my amendment.").

<sup>139</sup> *Merriken v. Cressman*, 364 F.Supp. 913, 916 (E.D. Pa. 1973) (all quotation marks and punctuation in original).

The argument that ensued was all about whether information sharing pursuant to these questionnaires lacked the consent conditions of voluntariness and/or knowledge—or, in the parlance of this article, was unavoidable. The school district argued that the challenged program, including the questionnaire, was voluntary, and therefore constitutional and within the discretionary power of the school board. But the plaintiffs asserted that there was no informed consent on behalf of the parents (i.e., insufficient knowledge), and that therefore the sharing of information was involuntary.<sup>140</sup> The court agreed with the plaintiffs that the program violated the right to privacy, resting its decision in part on the fact that the program did not obtain informed consent, thus depriving parents of the ability to avoid the information sharing.<sup>141</sup>

Senator Buckley expressed outrage that families were unable to avoid questionnaires and other information collection such as that at issue in *Merriken*, describing violations of privacy that “occur daily in schools across the Nation, through courses requiring the student to reveal personal data and feelings, and by means of demands by the Federal Government for personal information on students and parents.”<sup>142</sup> He went on to argue that “[t]he sense of a loss of control over one’s life and destiny . . . seems to be increasingly felt by parents with respect to the upbringing of their own children.”<sup>143</sup>

Thus was born the precursor to FERPA: the legislation then known as the “Buckley Amendment,” the design of which was to give control to parents so that information flows from schoolchildren would no longer be unavoidable. One of the stated five goals of the language as introduced by Senator Buckley was to “require parental consent or notification before their children are made to undergo certain forms of testing or partake in certain experimental or attitude-affecting programs or activities.”<sup>144</sup> Buckley said, “[m]y amendment simply gives individual parents the right to be informed about out-of-the-ordinary federally funded programs in which their child might participate, and assures the parents the right not to have their particular child participate if they find such a program objectionable.”<sup>145</sup>

In support of the legislation, Senator Ervin of North Carolina also hinted at the lack of voluntariness for children asked to complete questionnaires like the one at issue in *Merriken*, explaining, “Much of the controversy concerning these school records centers around the use of classroom questionnaires that are financed by governmental grants . . . . The situation now is that children are rarely given a free

---

<sup>140</sup> *Id.* at 917 (“The CPI program as presented above is considered by its advocates, the Defendants, as a voluntary program . . . . The Plaintiffs assert that the Program is not voluntary because individuals’ constitutional rights are waived without knowing.”).

<sup>141</sup> *Id.* at 920 (“any attempt at informed consent does not reach the level that this court would consider adequate as in the ‘consent ideally obtained by a physician prior to the performance of surgery’”); *id.* at 922 (stating as a conclusion of law that the program “will be administered without the knowing, intelligent, voluntary and aware consent of parents or students.”).

<sup>142</sup> 120 Cong. Rec. Senate 14,580 (May 14, 1974).

<sup>143</sup> *Id.*

<sup>144</sup> *Id.* at 14,581.

<sup>145</sup> *Id.*



and unprejudiced choice of answering or not answering the questionnaires.”<sup>146</sup> Senator Ervin entered into the record the transcript of a press conference held earlier that year by a coalition of Maryland parents, who also emphasized the compulsory and unavoidable nature of in-school information collections. In one “widespread example” invoked by the parent coalition, “the Maryland State Board of Education By-laws call for a compulsory treatment of subject matter known as Interpersonal Relationships. No child in public schools in the State of Maryland may be excused from these discussions and classroom activities.”<sup>147</sup> The parent coalition further pointed out that teachers could not refuse to administer invasive questionnaires, out of “fear of reprisal or dismissal from the public school system.”<sup>148</sup>

### G. Unavoidability in Section 5 of the FTC Act

A reference to “unavoidability” will, for many privacy scholars, immediately conjure Section 5 of the FTC Act. This is because Section 5 of the FTC Act is the closest thing in American law to a general federal consumer privacy law, and unavoidability is a central part of Section 5 analysis. The important role played by unavoidability in informing privacy policy set by the FTC thus is rather self-evident.

The FTC explicitly names unavoidability in its Section 5 unfairness analysis. A practice is considered unfair, and thus prohibited under Section 5, if it causes harm that: 1) is substantial, 2) is not outweighed by countervailing benefits to consumers or competition that the practice produces, and 3) cannot reasonably be avoided by consumers themselves.<sup>149</sup> According to J. Howard Beales, former director of the FTC’s Bureau of Consumer Protection, “If consumers could have made a different choice, but did not, the Commission should respect that choice.”<sup>150</sup>

Unavoidability is also a part of deception analysis. Deception is best viewed as a category of unfairness—as the FTC explained in *International Harvester*, “unfairness is the set of general principles of which deception is a particularly well-established and streamlined subset.”<sup>151</sup> Under the classic formulation of deception, the agency asks whether an entity made a misrepresentation or omission regarding a service or product, and whether the misrepresentation was “material,” or significant enough that it likely would have altered consumers’ behavior vis-à-vis the service or product if they had known the truth.<sup>152</sup>

---

<sup>146</sup> *Id.* at 14,585.

<sup>147</sup> *Id.* at 14,587.

<sup>148</sup> *Id.* at 14,586.

<sup>149</sup> FED. TRADE COMM’N, POL’Y STATEMENT ON UNFAIRNESS (Dec. 17, 1980), <https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness>.

<sup>150</sup> J. Howard Beales, FTC, *The FTC’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, May 30, 2003, <https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection>.

<sup>151</sup> *International Harvester*, 104 F.T.C. 949, 1060 (1984); see Beales *supra* note 150.

<sup>152</sup> FED. TRADE COMM’N, POL’Y STATEMENT ON DECEPTION (Oct. 14, 1983), [https://www.ftc.gov/system/files/documents/public\\_statements/410531/831014deceptionstmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf)

Visiting for a moment the unavailability factors discussed above—lack of voluntariness and lack of knowledge—the FTC’s Section 5 doctrine contemplates unavailability caused by a deficit in either of these areas. On lack of voluntariness, the FTC said in its policy statement on unfairness that it brings unfairness cases “to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision-making.”<sup>153</sup>

On lack of knowledge, Beales explained that the FTC considers consequences of a deception to be unavoidable because the consumer lacks sufficient knowledge to avoid those consequences, “precisely because the seller misled them about the consequences of the choice.”<sup>154</sup> The FTC observed in *International Harvester*, “[w]hether some consequence is ‘reasonably avoidable’ depends, not just on whether people know the physical steps to take in order to prevent it, but also on whether they understand the necessity of actually taking those steps.”<sup>155</sup> When the tractor maker accused of unfairness in that case argued that operators of its tractors could have avoided injury by following certain safety rules, the FTC countered, “[t]his argument presupposes that the operators of its tractors have the basic information necessary to avoid such injury.”<sup>156</sup>

The FTC also equated lack of knowledge with unavailability in its 2013 complaint against LabMD (the FTC’s order was later vacated by the 11th Circuit), when it found that LabMD’s data security failures constituted an unfair practice.<sup>157</sup> At the time, the agency stated, “Consumers have no way of independently knowing about respondent’s security failures and could not reasonably avoid possible harms from such failures.”<sup>158</sup>

The FTC has also considered retroactive changes to companies’ privacy policies or settings to be unfair, because customers have no way of knowing that the terms of their information sharing have changed.<sup>159</sup>

Outside of enforcement actions, the FTC has suggested that information shared under conditions lacking in voluntariness may be viewed with increased scrutiny by the agency, and in particular that the essential or important nature of a type of

---

<sup>153</sup> FED. TRADE COMM’N, *supra* note 149.

<sup>154</sup> J. Howard Beales, FTC, *The FTC’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, May 30, 2003, <https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection> (“consumers cannot reasonably avoid the injury precisely because the seller misled them about the consequences of the choice.”).

<sup>155</sup> *International Harvester*, 104 F.T.C. at 1066.

<sup>156</sup> *Id.* at 1043 (1984).

<sup>157</sup> Complaint, LabMD, Inc., F.T.C. Docket No. 9357 (Aug. 29, 2013), <https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf>.

<sup>158</sup> *Id.* at ¶12.

<sup>159</sup> *Gateway Learning Corp.*, 138 F.T.C. 443, 449 (2004) (stating that Gateway’s retroactive application of revised privacy policy to consumers’ information “was, and is, an unfair act or practice.”); *Facebook, Inc.*, FTC File No. 0923184, Docket No. C-4365 (F.T.C. July 27, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf>; see Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 640 (2011) (stating that “[a]ccording to the FTC, it is unfair to change the terms that govern personal information that was collected under a previous, different agreement.”).

service—as well as the amount of competition in an industry—may be relevant in privacy considerations. In a 2012 report on *Protecting Consumer Privacy in an Era of Rapid Change*, the FTC agreed with public commenters that a take-it-or-leave-it approach to privacy, in which a company makes consumers’ use of a product or service contingent upon consumers’ acceptance of specific data practices, “is problematic from a privacy perspective, in markets for important services where consumers have few options.”<sup>160</sup> A footnote offered the caveat that this position—and the report generally—were “not intended to reflect Commission guidance regarding Section 5’s prohibition on unfair methods of competition.”<sup>161</sup> But the FTC nevertheless went on to state that “[f]or such products or services, businesses should not offer consumers a ‘take it or leave it’ choice when collecting consumers’ information in a manner inconsistent with the context of the interaction between the business and the consumer.”<sup>162</sup> As an illustrative example, the FTC discussed broadband Internet access, observing both that broadband has become a critical service, and that consumers may have few options for broadband service.<sup>163</sup>

#### IV. POLICYMAKERS’ HISTORICAL PATTERN FOR ADDRESSING UNAVOIDABILITY

Across the several areas explored above, a pattern emerged. There were three primary rationales that policymakers saw fit to afford heightened protections to information shared unavoidably: to foster trust in certain services and relationships; to protect vulnerable individuals from harm; and to defend privacy as a matter of right on behalf of data subjects who cannot defend it themselves. To deliver on these rationales, when confronted with issues pertaining to information shared unavoidably, policymakers typically instituted a consent requirement, prohibiting the information from being further shared in the absence of permission from the subject.

##### A. Rationales for protecting information shared unavoidably

Three rationales for protecting information shared unavoidably appear repeatedly in the history of U.S. privacy law explored above. They are referred to in this article as the trust rationale, protection rationale, and right rationale.

##### 1. The trust rationale

The trust rationale holds that privacy protections are sometimes necessary to foster trust and confidence in relationships to facilitate desirable sharing of information. Without trust, some information would not be shared, and services

---

<sup>160</sup> FED. TRADE COMM’N, *Protecting Consumer Privacy in an Era of Rapid Change* 51 (2012).

<sup>161</sup> *Id.* at 51 n. 245.

<sup>162</sup> *Id.* at 51.

<sup>163</sup> *Id.* at 52.

would fail, commerce would suffer, or relationships and networks would not flourish to their fullest extent.

This rationale has been widely discussed in recent years. For example, Jessica Litman argued in 2000 that merchants, banks, and insurance companies encourage their customers to expect strong privacy protections from these institutions, surmising that “[w]ithout that trust, we’d be reluctant to volunteer our credit card numbers; we’d think twice before making embarrassing purchases or watching certain pay-per-view movies.”<sup>164</sup> In the privacy blueprint that it released in 2012, the White House asserted, “Privacy protections are critical to maintaining consumer trust in networked technologies.”<sup>165</sup> In their landmark 2016 article, *Taking Trust Seriously in Privacy Law*, Neil Richards and Woodrow Hartzog explained that “[b]ecause disclosure of personal data leaves people vulnerable, trust is the glue that holds together virtually every . . . relationship that requires personal information to develop or achieve a particular goal.”<sup>166</sup> And in his 2018 book on *Privacy as Trust: Information Privacy for an Information Age*, Ari Waldman asserted, “Trust gives us the confidence and willingness to share because it mitigates the vulnerabilities inherent to disclosure.”<sup>167</sup>

The concept of trust as a motivation for privacy law has been raised repeatedly throughout history in support of heightened privacy in several of the contexts of unavoidable information sharing explored above, particularly where essential services are concerned. To draw on and summarize relevant pieces in the historical exploration above, the trust rationale was alluded to since antiquity by physicians who spoke of being “entrusted with the secrets of the great”<sup>168</sup> and of the honor and reputation of the medical profession.<sup>169</sup> It was stated explicitly by the Department of Health and Human Services when it adopted the HIPAA Privacy Rule and stated that the “patient must trust the clinician” to use information for health-related purposes and also respect the need for privacy.<sup>170</sup> This rationale was also raised at common law in the 18th century regarding attorney-client communications when a need was recognized “to render it safe for clients to communicate to their attorneys”<sup>171</sup>—and continues to be acknowledged by the American Bar Association, which asserts that confidentiality “contributes to the trust that is the hallmark of the client-lawyer relationship.”<sup>172</sup> It has been acknowledged by the Federal

---

<sup>164</sup> Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1308 (2000).

<sup>165</sup> White House, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), available at <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>.

<sup>166</sup> Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 451–52 (2016).

<sup>167</sup> ARI EZRA WALDMAN, *PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE* 61 (2018).

<sup>168</sup> Letter from St. Jerome to Nepotian, *supra* note 46.

<sup>169</sup> See discussion *supra* p. 69.

<sup>170</sup> Standard for Privacy of Individually Identifiable Health Information, *supra* note 53.

<sup>171</sup> Annesley, 17 How. St. Trials at 1241.

<sup>172</sup> American Bar Association, *supra* note 63.

Communications Commission, which discussed the role of privacy in “bolster[ing] consumer trust” in telecommunications.<sup>173</sup> And it was discussed by courts in early cases regarding financial privacy, when judges compared the relationship between bankers and customers to that between attorneys and clients and stated that the “credit of the customer depends very largely upon the strict observance” of confidence.<sup>174</sup>

Maximizing participation in essential services has always been a popular policy goal, and innumerable policies exist and have been frequently revised to diminish barriers to essential services and to encourage people to adopt and use them. Privacy protections have been some of those policies. Perhaps this is why, in writing about physician-patient privilege in 1985, scholar Daniel W. Shuman described this rationale as the “utilitarian” or “instrumental” approach, “which considers the utility of a privilege to the relationship it seeks to protect and the relationship’s value to society.”<sup>175</sup> Relatedly, when John Henry Wigmore set forth four conditions that generally must be met for evidentiary privilege to attach to communications between two persons (attorney and client, priest and penitent, or spouses), one condition was that the “relation must be one which in the opinion of the community ought to be sedulously fostered.”<sup>176</sup>

There is clear evidence that the trust rationale is well-grounded—that when privacy protections do not sufficiently foster trust in essential services, people may not fully avail themselves of those services. As one reluctant patient told researchers in Canada, “You know, [doctors] want you to tell them everything . . . but I don’t want to tell you [doctors] this part, because I don’t trust you guys.”<sup>177</sup> And a 2003 review of studies of patient perspectives on medical privacy concluded that across multiple studies, one common finding was that

patients will delay or forego treatment, or alter stories about symptoms and onset of illness, to be sure those details never emerge publicly. Adolescents, battered women, people with HIV or those at high risk for HIV, women undergoing genetic testing, and mental health patients all reported at least occasional instances when they chose not to seek treatment because of confidentiality concerns, or decided to withhold information during clinical interactions for the same reason.<sup>178</sup>

---

<sup>173</sup> FED. TRADE COMM’N, *supra* note 88 at ¶ 37.

<sup>174</sup> Tournier, 1 KB at 461.

<sup>175</sup> Daniel W. Shuman, *The Origins of the Physician-Patient Privilege and Professional Secret*, 39 SW. L. J. 661, 663–664 (1985).

<sup>176</sup> Wigmore, *Treatise on Anglo-American System of Evidence in Trials at Common Law*, § 2285.

<sup>177</sup> Serena S. Small, Corinne M. Hohl, and Ellen Balka, *Patient Perspectives on Health Data Privacy and Implications for Adverse Drug Event Documentation and Communication: Qualitative Study*, J. MED. INTERNET RESEARCH (2021).

<sup>178</sup> Pamela Sankar, Susan Moran, Jon F. Merz, & Nora L. Jones, *Patient Perspectives on Medical Confidentiality: A Review of the Literature*, 18 J. GEN. INTERN. MED. 659, 666 (2003).

There is evidence that a lack of trust has tangible effects online as well. In 2015, Darren Stevenson and Josh Pasek reported statistical evidence that people with greater trust in online firms were much more likely to desire personalized content.<sup>179</sup> That same year, the Census Bureau collected data on computer and internet use for the National Telecommunications and Information Administration, which, upon processing the data, concluded that a lack of trust in online privacy and security was prompting some Americans to limit their online activity.<sup>180</sup> In 2016, Ari Waldman published a study of Facebook users' willingness to share intimate information on the platform, which found that among the variables examined, proxies for users' trust in the platform were the only statistically significant predictors of willingness to share.<sup>181</sup> And according to surveys conducted by the Ponemon Institute, after the Cambridge Analytica privacy fiasco, the percentage of Facebook users who agreed that "Facebook is committed to protecting the privacy of my personal information" fell from 79 percent to 27 percent.<sup>182</sup> Falling trust levels negatively affected usage of the service, with 9 percent saying they had already stopped using Facebook and 31 percent saying they were likely or very likely to use the service less or stop using it altogether.<sup>183</sup>

## 2. The protection rationale

The protection rationale holds that privacy protections are sometimes necessary to protect people from harms they may suffer as a result of sharing information, when they cannot avoid the initial information sharing. The American liberal tradition generally assumes that people will take steps to protect themselves and eschews paternalism. But when people cannot protect themselves, the law often steps in.

It is easy to understand why the protection rationale would have an important role to play in establishing privacy protections for information shared unavoidably. When circumstances frustrate voluntariness, an individual may find that they have to share information even though the sharing exposes them to risk of some harm. As a result, legal protection is necessary to reduce the risk of harm.

The protection rationale is of particular prominence in the FTC's body of work on privacy under its authority to enforce the FTC Act's prohibition against unfair

---

<sup>179</sup> Darren Stevenson & Josh Pasek, *Privacy Concern, Trust, and Desire for Content Personalization* (Mar. 30, 2015). TPRC 43: The 43rd Research Conference on Communication, Information and Internet Policy Paper, available at <https://ssrn.com/abstract=2587541>.

<sup>180</sup> Rafi Goldberg, U.S. National Telecommunications and Information Administration, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, U.S. Nat'l Telecomm. and Info. Admin. (May 13, 2016), <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>.

<sup>181</sup> Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RESRV. L. REV. 193, 218 (2016).

<sup>182</sup> Herb Wesiman, *Trust in Facebook Has Dropped by 66 Percent Since the Cambridge Analytica Scandal*, NBC News, Apr. 18, 2018, <https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011>.

<sup>183</sup> *Id.*

or deceptive practices in or affecting commerce.<sup>184</sup> Because, in the FTC's words, "[u]njustified consumer injury is the primary focus of the FTC Act," the agency will not step in to protect consumer privacy absent some potential harm that consumers must be protected from.<sup>185</sup> A finding of actual or likely injury to consumers thus is a necessary precondition for the FTC to find that a practice is unfair or deceptive.<sup>186</sup> The FTC assumes that consumers normally will be able to protect themselves from injury, and that it need only step in to protect them from injury when there is some reason that they otherwise cannot avoid it.<sup>187</sup>

### 3. The right rationale

Finally, the right rationale holds that privacy protections are necessary to defend people's right to privacy as a matter of justice and autonomy in situations where some other force prevents them from controlling their own information. Unavoidability is one such force.

The right rationale was described by Daniel W. Shuman in 1985, who wrote that one school of reasoning in support of the physician-patient privilege is the deontological or humanistic approach, which "focuses on the importance of the societal values ensconced within a privilege, arguing that disclosure of confidences revealed in certain relationships is in and of itself wrong."<sup>188</sup> In the words of medical ethicist Ian E. Thompson, because patients often appear before medical providers in a compromised state, "The moral responsibility of the doctor in the first instance is to respect the vulnerability of the 'patient'; his privacy in this sense."<sup>189</sup>

The right rationale was also alluded to repeatedly in the history of several of the areas of privacy law discussed above, often as policymakers made an emotional appeal to the need for heightened protections. It was raised in the discussions leading up to wiretap legislation, when Representative Beck decried the ability of government agents "to listen to everything you may say, messages of love and affection and of sacred confidence, or of the most intimate, confidential business."<sup>190</sup> It was alluded to by the Privacy Protection Study Commission and Congress in the 1970s when, for example, Representative Cavanaugh lamented the fact that, "the changing patterns of life took the possession of information about himself out of the control of the individual."<sup>191</sup> It was implied by a number of third-party doctrine cases in which courts examined whether individuals had "assumed

<sup>184</sup> 15 U.S.C. § 45.

<sup>185</sup> FED. TRADE COMM'N, *supra* note 149.

<sup>186</sup> FED. TRADE COMM'N, *supra* note 152 (stating that materiality is the same as injury); FED. TRADE COMM'N, *supra* note 149 (discussing substantial injury).

<sup>187</sup> FED. TRADE COMM'N, *supra* note 149 (discussing substantial injury).

<sup>188</sup> Daniel W. Shuman, *The Origins of the Physician-Patient Privilege and Professional Secret*, 39 SW. L. J. 661, 664 (1985).

<sup>189</sup> Ian E. Thompson, *The Nature of Confidentiality*, 5 J. MED. ETHICS 57, 59 (1979).

<sup>190</sup> 74 Cong. Rec. 2832 at 2902 (1931) (including remarks of Rep. Beck).

<sup>191</sup> *The Safe Banking Act: Hearings on H.R. 9086. 3 before the Subcomm. on Fin. Inst. Supervision, Regul., and Ins. of the Comm. on Banking, Fin., and Urb. Aff., 95th Cong. 1st Sess., pt. 3 at 1451 (1975) (including remarks of Rep. Cavanaugh).*

the risk” of downstream disclosure when they shared information with third parties.<sup>192</sup> And it was raised by Senator Buckley when pitching the legislative amendment that would eventually become FERPA—action was needed because “[t]he sense of a loss of control over one’s life and destiny . . . seems to be increasingly felt by parents with respect to the upbringing of their own children.”<sup>193</sup>

*B. How policymakers have protected information shared unavoidably*

Acting in service of the goals to foster trust, protect individuals from harm, and preserve a right with roots in justice and autonomy, policymakers often have found the solution to be relatively straightforward. First and perhaps most obviously: restore as much avoidability as possible in information sharing through rules establishing standards for transparency and consent. Second, protect against harm and foster trust by carefully restricting the processing of information for purposes other than that for which the information was unavoidably shared. This aligns with the analysis of the Privacy Protection Study Commission in 1977, which concluded that when information sharing is unavoidable because it is a condition precedent to “particular social, economic, or political relationships,” reliance on mere informed consent is invalid.<sup>194</sup> Under those circumstances, the Commission advised a policy requiring specific authorization, rather than consent, for disclosure, coupled with a “principle of limited disclosure.”<sup>195</sup>

The logical implementation of this two-part approach to protecting information shared unavoidably (first, restore avoidability; second, cabin processing) is a basic rule barring information shared unavoidably from being used other than as necessary to fulfill the purpose for which it was shared, unless the data subject provides consent.

An examination of the various types of unavoidable information sharing explored above reveals that this is, indeed, the general rule that policymakers have applied in several of those contexts. These are the privacy obligations placed on healthcare providers under HIPAA and the Code of Medical Ethics,<sup>196</sup> attorneys

---

<sup>192</sup> See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588 (2009).

<sup>193</sup> 120 Cong. Rec. 14392 at 14580 (1974) (including remarks of Senator Buckley).

<sup>194</sup> THE REP. OF THE PRIV. STUDY COMM’N, *Personal Privacy in an Information Society* at 19 (1977).

<sup>195</sup> *Id.* (emphasis in original).

<sup>196</sup> See HEALTH AND HUM. SERV. OFFICE FOR C.R., *Your Health Information Privacy Rights*, [https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer\\_rights.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf) (“Generally, your health information cannot be used for purposes not directly related to your care without your permission.”); see also CODE OF MED. ETHICS OP. 3.2.1 (AM. MED. ASS’N), <https://www.ama-assn.org/delivering-care/ethics/confidentiality>.



under their professional obligation of confidentiality,<sup>197</sup> educators under FERPA,<sup>198</sup> and telecommunications providers under the Communications Act.<sup>199</sup> Financial providers under GLBA must give their customers the opportunity to opt out of the sharing of information with nonaffiliated third parties in most situations other than when the information sharing is necessary to process a financial transaction requested or authorized by the customer.<sup>200</sup>

This approach operated relatively well on a sector-by-sector basis throughout much of the history of U.S. privacy law. However, as explained below, the sectoral implementation of this approach has become more challenging in recent decades.

#### V. PRECIPITOUS UNAVOIDABILITY AND THE CURRENT LEGISLATIVE DILEMMA

The historical and intuitive significance of unavoidability in U.S. privacy law helps explain the current legislative problem facing policymakers, and in particular how and why many recent legislative proposals on privacy include provisions not typically seen in U.S. privacy law, such as anti-discrimination protections. The current state of affairs is a natural response to the precipitous change in unavoidability that has occurred over the past few decades. Due to that change, in many instances avoidability simply cannot be restored. As a result, innovative new legislative proposals are attempts to deliver on the same trust rationale, protection rationale, and right rationale that have animated U.S. privacy law throughout its history, albeit in creative new ways that extend beyond the sectoral control-based approach that worked in the past.

---

<sup>197</sup> For example, under the ABA Model Rule on Confidentiality, “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b),” enumerating certain limited exceptions. MODEL RULES OF PROFESSIONAL CONDUCT, r. 1.6 (AM. BAR ASS’N), [https://www.americanbar.org/groups/professional\\_responsibility/publications/model\\_rules\\_of\\_professional\\_conduct/rule\\_1\\_6\\_confidentiality\\_of\\_information/](https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/).

<sup>198</sup> See U.S. DEP’T OF EDUC., *A Parent Guide to the Family Educational Rights and Privacy Act* (FERPA), [https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/A%20parent%20guide%20to%20ferpa\\_508.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/A%20parent%20guide%20to%20ferpa_508.pdf) (“Under FERPA, a school generally may not disclose PII from a student’s education records to a third party unless the student’s parent has provided prior written consent.”).

<sup>199</sup> 47 U.S.C. § 222 (c)(1) (1934) (“Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.”).

<sup>200</sup> See FED. TRADE COMM’N, *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, <https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act#obligations>.

### A. Precipitous unavailability in the digital era

The unavailability of information sharing changes dramatically over time, and we are living in a time of unavailability upheaval. Unavailable information sharing is exploding due to tremendous expansion of information shared in situations involving unavailable services, unavailable providers, and practical unavailability.

#### 1. The internet as an unavailable service

One major and perhaps obvious change that has happened over the past couple of decades is that the internet has become an unavailable service. The Infrastructure Investment and Jobs Act recently passed by Congress and signed into law recognizes that “access to affordable, reliable, high-speed broadband is essential to full participation in modern life in the United States.”<sup>201</sup> This reflects the widely held view of people in the U.S.—a survey conducted by the Pew Research Center in April 2021 found that 58% of U.S. adults said the internet was essential to them personally during the COVID-19 pandemic, and 90% said it was essential or important.<sup>202</sup> In addition, as mentioned above, since 2016, the United Nations has recognized freedom of expression online as a right,<sup>203</sup> and for several years, advocates and scholars have argued that broadband should be regulated as a utility.<sup>204</sup>

The essential nature of internet connectivity means, of course, that individuals cannot avoid sharing their information with internet service providers. The Federal Communications Commission discussed this at length in 2015 and 2016 and attempted to address it by promulgating privacy rules that would have applied to broadband providers, but were later vacated by Congress. The FCC issued a fact sheet alongside the rules that explained, “ISPs serve as a consumer’s ‘on-ramp’ to the Internet. Providers have the ability to see a tremendous amount of their customers’ personal information that passes over that Internet connection, including their browsing habits.”<sup>205</sup>

The fact that individuals’ lives have necessarily moved online also means that everyday conduct results in digital interactions with innumerable entities that wish

<sup>201</sup> 47 U.S.C. § 1701(1) (2021).

<sup>202</sup> See Colleen McClain et al., PEW RSCH. CTR, *THE INTERNET AND THE PANDEMIC* at 3 (2021), <https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/>.

<sup>203</sup> See U.N. GAOR, A/HRC/RES/32/13, [https://www.article19.org/data/files/Internet\\_Statement\\_Adopted.pdf](https://www.article19.org/data/files/Internet_Statement_Adopted.pdf); see also Catherine Howell & Darrell M. West, *The Internet as a Human Right*, BROOKINGS INST. (Nov. 7, 2016), <https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/>.

<sup>204</sup> See, e.g., Susan Crawford, *Why Broadband Should Be a Utility*, BROADBAND COMMUNITIES MAG. Mar.–Apr. 2019, <https://www.bbcmag.com/law-and-policy/why-broadband-should-be-a-utility>.

<sup>205</sup> FED. TRADE COMM’N, *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice Over Their Personal Information* (Nov. 2, 2016), <https://docs.fcc.gov/public/attachments/DOC-341938A1.pdf>; see FED. TRADE COMM’N, *supra* note 88, at ¶ 296 (“broadband plays a pivotal role in modern life”).

to collect and use some information about the individual shared through use of a connected device, online service, and/or app. The technically sophisticated may be accustomed to thinking of these as many different interactions with numerous providers of a variety of services, but as discussed below, this approach is not sustainable as a practical matter.<sup>206</sup>

Instead, as connectivity grows ubiquitous, it seems natural to shift cognitively toward thinking of digital interactions online as monolithic. There are indications that this shift is taking place. For example, when the Supreme Court found that warrantless tracking of a person's car using a device surreptitiously attached to the car violated the Fourth Amendment in *U.S. v. Jones*, Justice Sotomayor, in her concurrence, reflected on the implications of people's growing dependence on technology that generates digital information, arguing,

[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach 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.<sup>207</sup>

In the words of Ari Waldman, “[t]here is . . . very little that is truly free about much of our disclosures on the Internet. . . . Much of that sharing is impossible to avoid if we hope to participate in modern life. And because it is done out of necessity, it cannot truly be a matter of free choice.”<sup>208</sup>

## 2. The rise of unavoidable digital providers

In the modern information economy, individuals also increasingly find themselves encountering—and being forced to share information with—unavoidable providers. In particular, a select small group of tech giants have become unavoidable. In the words of Julie Cohen, “the platform business model is an undeniable commercial success.”<sup>209</sup> A few such platforms have been so successful and become so dominant that they are now unavoidable for anyone who uses the Internet—an essential service.<sup>210</sup> As a result of this shift toward centralized and dominant platforms, Cohen observes that “the everyday lives of network users have become increasingly datafied—converted into structured flows of data suitable for continuous collection and analysis at the platform level.”<sup>211</sup> This section

<sup>206</sup> See *infra* Section IV(a)(3) (discussing “the growth of practical unavoidability”).

<sup>207</sup> *United States v. Jones*, 565 U.S. 400, 417 (2012) (internal citations omitted).

<sup>208</sup> Ari Ezra Waldman, *PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE* at 67–68 (2018).

<sup>209</sup> Julie E. Cohen, *Law for the Platform Economy*, 51 U.C.D. L. REV. 133, 142 (2017).

<sup>210</sup> See Charlotte Slaiman, *Why Dominant Digital Platforms Need More Competition: Tech Giants Hold Special Positions in the Market; They Are Unavoidable*, CTR. FOR INT’ S GOVERNANCE INNOVATION, <https://www.cigionline.org/articles/why-dominant-digital-platforms-need-more-competition/>.

<sup>211</sup> Julie E. Cohen, *Law for the Platform Economy*, 51 U.C.D. L. REV. at 140.

discusses three specific providers that have become practically unavoidable: Google, Amazon, and Facebook.

To test the unavoidability of particular providers, in late 2018 journalist Kashmir Hill tried to cut Amazon, Facebook, Google, Microsoft, and Apple out of her life over the course of five weeks.<sup>212</sup> She concluded that, with the exception of Apple, it was impossible to avoid the companies completely.<sup>213</sup> “These companies are unavoidable because they control internet infrastructure, online commerce, and information flows,” she wrote.<sup>214</sup> A reader commented on her writeup for the *New York Times*, “Exactly! That is the point - we can’t avoid using the products/services of these giant companies.”<sup>215</sup>

Just by using the internet, any user almost certainly subjects himself to tracking by Google. According to research conducted by Timothy Libert in 2015, at that time, Google was able to track users on nearly 8 of 10 sites in the top one million websites (as determined by Alexa).<sup>216</sup> The following year, Steven Englehardt and Arvind Narayanan performed an in-depth examination of online tracking on the top 1 million websites and found that “[a]ll of the top 5 third parties [engaged in tracking on these websites], as well as 12 of the top 20, are Google-owned domains.”<sup>217</sup>

In addition, about 46% of U.S. smartphone users have phones that run Google’s Android operating system.<sup>218</sup> All but 0.35% of smartphone users are running either Android or Apple’s iOS,<sup>219</sup> so as a practical matter, in order to have a smartphone, a consumer cannot avoid sharing information with one of these two companies. But for many low-income consumers, Android is the only available option because the least expensive smartphones are Android devices.<sup>220</sup> And Google has been plagued

---

<sup>212</sup> See Kashmir Hill, *I Cut the ‘Big Five’ Tech Giants From My Life. It Was Hell*, GIZMODO (Feb. 7, 2019), <https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194>; see also Kashmir Hill, *I Tried to Live Without the Tech Giants. It Was Impossible.*, N.Y. TIMES (July 31, 2020), <https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html>.

<sup>213</sup> Kashmir Hill, *I Tried to Live Without the Tech Giants. It Was Impossible.*, N.Y. TIMES (July 31, 2020), <https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html>.

<sup>214</sup> Kashmir Hill, *I Cut the ‘Big Five’ Tech Giants From My Life. It Was Hell*, GIZMODO (Feb. 7, 2019), <https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194>.

<sup>215</sup> Hill, *supra* note 211.

<sup>216</sup> Timothy Libert, *Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites*, 9 INTL. J. COMM. 3544, 3545 (2015).

<sup>217</sup> Steven Englehardt & Arvind Narayanan, *Online Tracking: 1-Million-Site Measurement and Analysis*, 23rd ACM CONF. ON COMPUT. AND COMM’N (2016), [https://www.cs.princeton.edu/~arvindn/publications/OpenWPM\\_1\\_million\\_site\\_tracking\\_measurement.pdf](https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf).

<sup>218</sup> *Market Share of Mobile Operating Systems in North America from January 2018 to June 2021*, STATISTA (June 30, 2021), <https://www.statista.com/statistics/1045192/share-of-mobile-operating-systems-in-north-america-by-month/>.

<sup>219</sup> *Id.*

<sup>220</sup> See Simon Hill and Mark Jansen, *Android vs. iOS: Which smartphone platform is the best?*, DIGITAL TRENDS, Apr. 14, 2021, <https://www.digitaltrends.com/mobile/android-vs-ios/>; see

by reports that it collects vast amounts of information about device users, often in contravention of users' preferences. In 2017, an investigation by Quartz revealed that Android phones were collecting the addresses of nearby cellular towers and sending that data back to Google, even when location services were disabled.<sup>221</sup> In 2018, an investigation by the Associated Press similarly found that Google services on both Android devices and iPhones were storing location data even when users had turned off "Location History" in their Google settings.<sup>222</sup> And Google has also been sued for its tracking behavior vis-à-vis Android users: by Arizona in 2020 and by Austrian privacy activist Max Schrems in 2021.<sup>223</sup>

Google has also been steadily cultivating dominance in the education market, and millions of students and teachers now find sharing information with Google unavoidable because they are required to use Google devices and services for school.<sup>224</sup> In 2017, Natasha Singer of the *New York Times* reported that more than half of primary- and secondary-school children in the U.S. were using Google education apps.<sup>225</sup> The company's presence in the education market has continued to grow since then. In January of 2019, Google reported that eighty million students and educators worldwide were using its productivity software for educational institutions.<sup>226</sup> In two years, this number had ballooned to 170 million.<sup>227</sup> In January of 2020, forty million Chromebooks were in use by students and educators,<sup>228</sup> and that was before the COVID-19 pandemic drove sales for Chromebooks and other

---

also Christopher Soghoian: *Your Smartphone Is a Civil Rights Issue*, TED CONF.(June 2016), [https://www.ted.com/talks/christopher\\_soghoian\\_your\\_smartphone\\_is\\_a\\_civil\\_rights\\_issue/](https://www.ted.com/talks/christopher_soghoian_your_smartphone_is_a_civil_rights_issue/).

<sup>221</sup> Keith Collins, *Google Collects Android Users' Locations Even When Location Services Are Disabled*, QUARTZ (Nov. 21, 2017), <https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled>.

<sup>222</sup> Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, ASSOCIATED PRESS (Aug. 13, 2018), <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb>.

<sup>223</sup> Tony Romm, *Arizona sues Google over allegations it illegally tracked Android smartphone users' locations*, WASH. POST (May 27, 2020), <https://www.washingtonpost.com/technology/2020/05/27/google-android-privacy-lawsuit/>; Javier Espinoza, *Max Schrems Accuses Google of Illegally Tracking Android Users*, FINANCIAL TIMES (Apr. 7, 2021), <https://www.ft.com/content/4617cc99-3ed2-49e1-b97f-db4f1b45b5db>.

<sup>224</sup> See Natasha Singer, *How Google Took Over the Classroom*, N.Y. TIMES (May 13, 2017), <https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html>.

<sup>225</sup> *Id.*

<sup>226</sup> John Vamvakitis, *Around the World and Back with Google for Education*, GOOGLE BLOG (Jan. 22, 2019), <https://www.blog.google/outreach-initiatives/education/around-the-world-and-back/>.

<sup>227</sup> Shantanu Sinha, *More Options for Learning with Google Workspace for Education*, GOOGLE BLOG (Feb. 17, 2021), <https://www.blog.google/outreach-initiatives/education/google-workspace-for-education/>.

<sup>228</sup> Jim Deno, *Improving 40 million Chromebooks for education*, GOOGLE BLOG (Jan. 21, 2020), <https://www.blog.google/outreach-initiatives/education/2020-chromebooks/>.

tools and services used for remote learning through the roof—four times more Chromebooks were sold in 2020 than in the previous year.<sup>229</sup>

Many workers also now find information sharing with Google unavoidable, because their employers have adopted Google services at the organizational level. In April 2019, Google reported that more than five million paying businesses were using its productivity software, including large companies such as Verizon, which at the time had over 130,000 employees.<sup>230</sup> As of April of 2021, 375,000 organizations in more than sixty countries were using its software tools for nonprofits.<sup>231</sup>

Some of Google's services have also become so dominant as to be largely unavoidable. For example, Google Maps is now used by 81% of websites that contain and/or use maps.<sup>232</sup>

Amazon is extremely difficult to avoid due not only to its massive size, but also the breadth of its services. As Lina Khan, now the Chair of the Federal Trade Commission, wrote in a 2017 landmark article about Amazon's meteoric rise into dominance across numerous markets,

In addition to being a retailer, it is a marketing platform, a delivery and logistics network, a payment service, a credit lender, an auction house, a major book publisher, a producer of television and films, a fashion designer, a hardware manufacturer, and a leading provider of cloud server space and computing power.<sup>233</sup>

Amazon is putting local retailers and booksellers out of business, limiting offline options for consumers to purchase certain goods. The platform is also positioning itself as the platform through which cities, counties, and schools purchase office and classroom supplies, leaving retailers with little choice other than to use Amazon to reach government buyers.<sup>234</sup>

---

<sup>229</sup> Mitchell Clark, *Chromebooks Just Had Their Best Year Ever*, THE VERGE (Jan. 30, 2021), <https://www.theverge.com/2021/1/30/22256873/chromebook-best-year-ever-double-yearly-sales>.

<sup>230</sup> David Thacker, *5 Million and Counting: How G Suite Is Transforming Work*, GOOGLE CLOUD (Feb. 4, 2019), <https://cloud.google.com/blog/products/g-suite/5-million-and-counting-how-g-suite-is-transforming-work>; *Number of Employees at Verizon from 2007 to 2020*, STATISTA (Feb. 2021), <https://www.statista.com/statistics/257304/number-of-employees-at-verizon/>.

<sup>231</sup> Abner Li, *G Suite for Nonprofits gets Google Workspace Rebrand with Discounted Upgrade Plans*, 9TO5GOOGLE (Apr. 12, 2021, 7:54 AM), <https://9to5google.com/2021/04/12/google-workspace-for-nonprofits/>.

<sup>232</sup> Maps Usage Distribution in the Top 1 Million Sites, BUILTWITH, <https://trends.builtwith.com/mapping/maps> (last visited July 19, 2021).

<sup>233</sup> Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 713 (2017).

<sup>234</sup> Olivia LaVecchia & Stacy Mitchell, AMAZON'S NEXT FRONTIER: YOUR CITY'S PURCHASING, INSTITUTE FOR LOCAL SELF-RELIANCE (July 2018), [https://ilsr.org/wp-content/uploads/2018/07/ILSR\\_AmazonsNextFrontier\\_Final.pdf](https://ilsr.org/wp-content/uploads/2018/07/ILSR_AmazonsNextFrontier_Final.pdf); Abha Bhattarai, *How Amazon's Contract to Sell Office Supplies to Cities Could Hurt Local Retail*, WASH. POST, July 10, 2018, <https://www.washingtonpost.com/business/2018/07/10/amazon-now-sells-office-supplies-books-thousands-cities-other-local-organizations/>.

Amazon is extremely difficult to avoid in part because it runs the internet's largest cloud provider, Amazon Web Services. In the first quarter of 2021, Amazon held a 32% share of the global market for cloud infrastructure.<sup>235</sup> As a result, Hill was able to stop shopping on Amazon, but she learned that "Amazon is deeply embedded in [her] life." She wrote, "I use it repeatedly every single day whether I realize it or not. Without it, I cannot function normally."<sup>236</sup> When she cut Amazon Web Services out of her life, some of the things that stopped working were various websites (including those of government agencies), the vacation property service Airbnb, the game Words With Friends, streaming services Netflix and HBO Go, the communication platform Slack, and the encrypted messaging app Signal.<sup>237</sup> A colleague helped block her access to Amazon's servers, but found that her devices tried to ping Amazon's servers nearly 300,000 times in one week.<sup>238</sup> Hill also found it difficult to avoid Amazon in the physical world, reporting that when she ordered an item from eBay, the seller used "Fulfillment by Amazon" to store and ship the product.<sup>239</sup>

Facebook, another tech giant, has become unavoidable for many users due to the platform's lack of competitive alternatives and network effects.<sup>240</sup> An individual user is theoretically free to leave whenever they like, but will find that it is not possible to replicate their network of friends and communities elsewhere.<sup>241</sup> As one user, a community organizer who moderates a 7000-person Facebook group, told the *Washington Post*, "I don't know how you could even transfer a fifth of the people [to another platform]."<sup>242</sup> The social network is particularly unavoidable for people compelled to get in touch with other people with something rare in common, such as a rare medical condition.<sup>243</sup>

Many people also report that they have no choice but to utilize the tech giants' platforms for professional reasons. For example, journalists may need Facebook's platform to get in touch with sources, freelancers to identify opportunities and clients, and marketing professionals to manage their employers' online presence.<sup>244</sup> But in addition to that, many people may feel compelled to establish and maintain

---

<sup>235</sup> Felix Richter, *Amazon Leads \$150-Billion Cloud Market*, STATISTA, July 5, 2021, <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>.

<sup>236</sup> Kashmir Hill, *I Tried to Block Amazon From My Life. It Was Impossible*, GIZMODO, Jan. 22, 2019, <https://gizmodo.com/i-tried-to-block-amazon-from-my-life-it-was-impossible-1830565336>.

<sup>237</sup> *Id.*

<sup>238</sup> *Id.*

<sup>239</sup> *Id.*

<sup>240</sup> See, e.g., Heather Kelly, *Why It's Easy to Hate Facebook but Hard to Leave*, WASH. POST, Nov. 19, 2020, <https://www.washingtonpost.com/technology/2020/11/19/can-not-quit-facebook/>.

<sup>241</sup> *Id.*

<sup>242</sup> *Id.*

<sup>243</sup> *Id.*

<sup>244</sup> Lydia Emmanouilidou & Brandi Fullwood, *We Asked Listeners Why They Can't Quit Facebook. Here's What You Said*, THE WORLD (Feb. 4, 2019), <https://www.pri.org/stories/2019-02-04/we-asked-listeners-why-they-cant-quit-facebook-heres-what-you-said>.

a Facebook account simply because having one is viewed as “normal” by potential employers. CareerBuilder reported in 2018 that 47 percent of employers said that if they can’t find a job candidate online, they are less likely to call that person in for an interview.<sup>245</sup> In one specific anecdote, a Navy veteran in Oregon applied for a job with a large national company and found that the job application requested information about candidates’ Facebook accounts. He didn’t have one, so he left the space blank. When he heard back from the company, he was told that he needed to get a Facebook account in order to be interviewed.<sup>246</sup>

### 3. The growth of practical unavailability

Alongside the proliferation of information sharing events due to the rise of the Internet as an unavoidable service and the growing unavailability of a handful of giant digital providers, unavoidable information sharing due to practical unavailability has also seen a dramatic shift in the digital era. Individuals increasingly find information sharing unavoidable as a practical matter due to a lack of information available to and processable by the average individual.

Professor Daniel Solove breaks this problem down effectively in his exposition on the failure of privacy self-management.<sup>247</sup> A variety of cognitive problems impair individuals’ ability to be informed about the costs and benefits of requested collection and use of their data and to make decisions that reflect their preferences.<sup>248</sup> In addition, there are too many entities collecting and using data to be individually managed, and there are too many unknowns of downstream uses and aggregation to reliably project costs and benefits.<sup>249</sup>

As lives increasingly are carried out online, a natural consequence is that individuals will lack an understanding of how their data is collected and used due to the sheer volume of information they would have to access and process to develop this understanding. Research conducted by Pew Research Center in early 2021 found that 31% of U.S. adults said they were online “almost constantly,” and 48% said they went online several times a day.<sup>250</sup> As discussed above, being online is now recognized as essential.<sup>251</sup> And for the average connected individual, everyday conduct results in digital interactions with innumerable entities that wish

---

<sup>245</sup> Landan Hayes, *Not Getting Job Offers? Your Social Media Could Be the Reason*, CAREERBUILDER, Aug. 9, 2018, <https://www.careerbuilder.com/advice/not-getting-job-offers-your-social-media-could-be-the-reason>.

<sup>246</sup> Laura Fosmire, *Senate Moves Forward on Social Media and Employment Bill*, STATESMAN J., Mar. 4, 2015, <https://www.statesmanjournal.com/story/money/business/2015/03/04/senate-moves-forward-social-media-employment-bill/24359757/>.

<sup>247</sup> See generally Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

<sup>248</sup> *Id.* at 1883–88.

<sup>249</sup> *Id.* at 1888–93.

<sup>250</sup> Andrew Perrin & Sara Atske, *About Three-in-Ten U.S. Adults Say They Are ‘Almost Constantly’ Online*, Pew Research Center, Mar. 26, 2021, <https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/>.

<sup>251</sup> See discussion *supra* Section 1.



to collect and use some information about the individual shared through use of a connected device, online service, and/or app.

This means that most individuals would, as a practical matter, never be able to meaningfully consider the information practices of various entities and exercise choices that reflect their preferences and beliefs. In 2008 Aleecia McDonald and Lorrie Faith Cranor estimated that at that time it would take an individual an average of 244 hours each year—the equivalent of six weeks of full-time work—to read the privacy policy of every new site visited.<sup>252</sup> Our lives have only moved more online since then, and recent research indicates that most people have come to accept, resignedly, that they cannot actually control their personal information. Survey research led by Joseph Turow a few years ago found that 58% of respondents both desired control over what marketers could learn about them online and had come to accept that they had little control over what marketers could learn about them.<sup>253</sup> As a result, Dennis Hirsch has argued that big data privacy harms “fall squarely” into a category of harms that consumers themselves cannot reasonably avoid, observing “[f]ew consumers can become aware of and achieve control over the collection of their personal information. Fewer still can understand how companies use data analytics to infer additional information about them and make decisions that affect them.”<sup>254</sup>

Even if individuals were generally capable of reading and processing details about how they will be tracked and their information used, privacy policies, which are presumed to communicate these things, often do not effectively do so.<sup>255</sup> Several years ago a team of legal scholars tested both experts’ and non-experts’ interpretations of a number of privacy policies and reported that their “findings suggest that privacy policies are written ambiguously and in a way that leads both knowledgeable users and crowd workers to misapprehend websites’ data practices as well as cause disagreement among experts with respect to certain data practices.”<sup>256</sup> The results of a 2019 survey conducted by the Pew Research Center support this finding: when asked how well they understand privacy policies, only 13% of respondents said they understand policies “a great deal,” with the remaining 87% saying they understood privacy policies only “some,” “very little,” or “none.”<sup>257</sup> When *New York Times* journalist Kevin Litman-Navarro analyzed the length and readability of privacy policies from nearly 150 popular websites and

<sup>252</sup> Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL’Y FOR INFO. SOC’Y 1, 17, 19 (2008), <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf> (estimating the national opportunity cost for the time it would take Americans to read every privacy policy they come across at \$781 billion).

<sup>253</sup> Joseph Turow et al., *The Tradeoff Fallacy* 14 (2015).

<sup>254</sup> Dennis D. Hirsch, *That’s Unfair! Or Is It? Big Data, Discrimination, and the FTC’s Unfairness Authority*, 103 KENTUCKY L. J. 345, 354 (2015).

<sup>255</sup> See generally Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users’ Understanding*, 30 BERKELEY TECH. L. J. 39 (2015).

<sup>256</sup> *Id.*

<sup>257</sup> Brooke Auxier et al., *Americans’ Attitudes and Experiences with Privacy Policies and Laws*, PEW RESEARCH CENTER, Nov. 15, 2019, <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/>.

apps, he concluded that on the whole, the policies were “an incomprehensible disaster.”<sup>258</sup>

Data collectors have an incentive to write privacy policies that offer little clarity about their practices because doing so creates legal coverage for a wide range of behavior. Discussing a decade-old conversation with someone who crafted privacy policies for companies, journalist Charlie Warzel recalls, “where you’re clicking ‘I Accept’ on the policy . . . he imagines a big boardroom. . . . On the other side of the table is a team of 30 highly paid Ivy League lawyers. . . . It’s that versus a vaguely disinterested person who’s like, ‘I just want this app to load now.’”<sup>259</sup>

But increasingly, privacy policies are actually beside the point. Individuals’ information choices are deeply manipulable and manipulated. Disclosures and information-collecting interfaces can be designed to guide individuals to the choices that data collectors want them to make.<sup>260</sup> For example, Alessandro Acquisti and others at Carnegie Mellon have done extensive work illustrating that contextual aspects of an information sharing, such as how and when an individual is asked to share information and informed about how that information will be used, can be shaped to alter the choices that individuals make.<sup>261</sup> For example, in one experiment, a team at Carnegie Mellon demonstrated that when data subjects were presented with misdirections during an information collection process, they made different disclosure decisions.<sup>262</sup> Acquisti et al. point out that many data collectors “respond to, and to a great extent exploit” the psychological characteristics and vulnerabilities of individuals to achieve a particular outcome.<sup>263</sup>

The result is, to put it bluntly, an increasingly plain failure of the so-called “notice and consent” framework to render the sharing of information in any given context avoidable. As Julie Cohen points out, privacy in a rich online world appears to be operationalized by notice and consent mechanisms, but

As a practical matter . . . information businesses have powerful incentives to configure the world of networked digital artifacts in ways that make enrollment seamless and near-automatic. Even when users do have choices to prevent collection of certain types of data, the design of user interfaces, menu options, and accompanying disclosures systematically obscures those choices, guiding users

---

<sup>258</sup> Kevin Litman-Navarro, *supra* note 29.

<sup>259</sup> Charlie Warzel, *supra* note 17.

<sup>260</sup> See Ryan Calo, *Digital Market Manipulation*, 82 G.W. L. REV. 995, 1004 (2014) (explaining that “firms can and do design every aspect of the interaction with the consumer”).

<sup>261</sup> See Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, *Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age*, 30 J. CONSUMER PSYCH. 736, 741 (2020).

<sup>262</sup> See Idris Adjerid, Alessandro Acquisti, Laura Brandimarte, & George Loewenstein, *Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency*, SOUPS ’13: PROCEEDINGS OF THE NINTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY, July 2013.

<sup>263</sup> See Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, *Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age*, 30 J. Consumer Psych. 736, 746 (2020).

instead toward options that involve more intensive data extraction. And many important details about the kinds of behavioral data that the sensing net extracts simply are not disclosed to users at all. Within the sensing net, practices of data are continuous, immanent, complex, and increasingly opaque to ordinary users.<sup>264</sup>

The hard truth is that to the questionable extent that individuals ever were capable of understanding how their information would be collected and used and expressing their preferences through privacy choices, they no longer are.

*B. Precipitous unavailability and the failure of the incumbent policy framework*

Due to the massive changes in unavoidable services, unavoidable providers, and practical unavailability that have occurred in recent decades, individuals now find that they are constantly sharing information about themselves in countless ways they cannot avoid. As discussed above, policymakers typically have approached unavailability by first attempting to restore avoidability, and second, restricting the information shared unavoidably from being used for purposes other than that for which it was collected. But this incumbent framework no longer is sufficient because there are now many instances in which avoidability simply cannot be restored. This failure has been discussed for years. It is not new; numerous scholars have explored the topic. For example, Dan Solove observed in 2013, “individuals cannot adequately self-manage their privacy, and consent is not meaningful in many contexts involving privacy.”<sup>265</sup> Neil Richards and Woodrow Hartzog have explored the “pathologies of consent”—the many ways in which even apparent consent can be illusory—and, documenting the widespread nature of these pathologies, concluded that the consent-based approach in the U.S. has been “a spectacular failure.”<sup>266</sup> Julie Cohen stated in 2019, “notice-and-consent protections . . . simply do not work.”<sup>267</sup> Woodrow Hartzog testified before the Senate Commerce Committee that same year that “notice and choice is irreparably broken.”<sup>268</sup>

This new reality is largely responsible for policymakers’ current struggle to craft appropriately responsive policy. As explored above, historically the goals of establishing protections for information shared unavoidably have been to foster trust in services and relationships, protect vulnerable individuals from harm, and defend privacy as a matter of right on behalf of data subjects who cannot defend it themselves. But because the incumbent framework can no longer achieve these

---

<sup>264</sup> JULIE E. COHEN, *BETWEEN TRUTH AND POWER* 58 (2019).

<sup>265</sup> Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1894 (2013).

<sup>266</sup> Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1498 (2019).

<sup>267</sup> Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES IN LAW 1, 6 (2019).

<sup>268</sup> Prepared Testimony and Statement for the Record of Woodrow Hartzog before the Senate Committee on Commerce, Science, and Transportation regarding “Policy Principles for a Federal Data Privacy Framework in the United States” at 3 (Feb. 27, 2019).

goals, policymakers are finding that they must go back to the drawing board and develop new and innovative solutions.

Accordingly, legislative proposals have recently emerged with creative and sweeping new frameworks that depart significantly from the sectoral control-based approach that worked in the past and that attempt to deliver on the three goals of legislating to protect information shared unavoidably.

To restore trust, recent comprehensive privacy bills supported by legislators of both major parties generally have had sweeping cross-sectoral coverage, and included provisions restricting uses—especially downstream uses—of collected information.<sup>269</sup>

To protect vulnerable individuals from harm, some recent bills have attempted to shore up privacy protections for broad categories of data viewed as particularly “sensitive”—often meaning most clearly connected to potential financial, physical, or reputational harms—across sectors,<sup>270</sup> a stark difference from older privacy laws that typically focus on data shared in particular contexts but decline to restrict that same type of data when it exists outside of the covered context. Some bills have taken on particular data-driven harms. For example, recent comprehensive privacy bills supported by legislators of both major parties generally have included provisions that would in some way address data-driven discrimination.<sup>271</sup> Other bills have more narrowly taken on and attempted to rein in harms that include

---

<sup>269</sup> See, e.g., American Data Privacy and Protection Act, H.R. 8152, 117<sup>th</sup> Cong. (2022) (“A covered entity or a service provider may not collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability.”); SAFE DATA Act, S. 2499, 117<sup>th</sup> Cong. (2021) (buttressing existing federal civil rights laws, enlisting the support of the FTC to refer possible violations to other agencies, and ordering the FTC to conduct a study of algorithmic discrimination); Consumer Online Privacy Rights Act, S. 3195, 117<sup>th</sup> Cong. (2021) (prohibiting the use of covered data to facilitate discriminatory advertising or eligibility determinations in the areas of housing, employment, credit, and education opportunity).

<sup>270</sup> See, e.g., Health and Location Data Protection Act of 2022, S. 4408, 117<sup>th</sup> Cong. (2022) (making it “unlawful for a data broker to sell, resell, license, trade, transfer, share, or otherwise provide or make available” an individual’s location data, health data, or other types of data that can reveal location or health); My Body, My Data Act of 2022, H.R. 8111, 117<sup>th</sup> Cong. (2022) (restricting the collection, retention, use, and disclosure of personal reproductive or sexual health information); Public Health Emergency Privacy Act, S. 81, 117<sup>th</sup> Cong. (2021) (imposing privacy, confidentiality, and security requirements on the use and disclosure of COVID-19 health data);

<sup>271</sup> See, e.g., H.R. 8152 - American Data Privacy and Protection Act (“A covered entity or a service provider may not collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability.”); S. 2499 - SAFE DATA Act (buttressing existing federal civil rights laws, enlisting the support of the FTC to refer possible violations to other agencies, and ordering the FTC to conduct a study of algorithmic discrimination); S. 3195 - Consumer Online Privacy Rights Act (prohibiting the use of covered data to facilitate discriminatory advertising or eligibility determinations in the areas of housing, employment, credit, and education opportunity).

manipulative online design practices,<sup>272</sup> algorithmic discrimination,<sup>273</sup> and the display of harmful online content (such as content promoting eating disorders, self-harm, and suicide) to kids and teens.<sup>274</sup>

To defend privacy as a matter of right on behalf of data subjects who cannot defend it themselves, comprehensive privacy legislation has included cross-sectoral individual privacy rights, typically including rights of access, correction, and deletion.<sup>275</sup> Other legislative efforts have attempted to restore individual rights against the persistent storage, aggregation, and downstream use and dissemination of information about themselves. For example, one bill would restrict law enforcement agencies' ability to obtain, share, and use as evidence certain types of information acquired from data brokers without a warrant.<sup>276</sup> Another would require data brokers to register with the FTC, and then create a process whereby individuals could request that data brokers delete their information.<sup>277</sup>

Although these efforts differ in many ways from the existing body of U.S. privacy law, they are in fact consistent with patterns found in the historical approach to unavailability in information sharing.

## VI. CONCLUSION

In discourse regarding the existing body of U.S. privacy law, there is wide recognition that policymakers care, ought to care, and historically have cared about factors such as the norms and expectations of information subjects; the degree of sensitivity of the information shared; and the severity of direct and tangible harms, such as identity theft. But a careful historical examination of several areas of U.S. privacy law reveals that another critically important but long-underappreciated factor has been at play all along: the degree to which a particular sharing of information is or is not unavoidable by the data subject.

Bringing the significance and important historical role of unavailability into the foreground helps explain both the momentousness of policymakers' current struggle to pass new privacy legislation, as well as why so many recent legislative proposals depart significantly from old models that focused on control-based mechanisms confined to specific sectors.

---

<sup>272</sup> See DETOUR Act, S. 3330, 117<sup>th</sup> Cong. (2021).

<sup>273</sup> See Algorithmic Accountability Act of 2022, S. 3572, 117<sup>th</sup> Cong. (2022); Algorithmic Accountability Act of 2022, H.R. 6580, 117<sup>th</sup> Cong. (2022).

<sup>274</sup> Kids Online Safety Act, S. 3663, 117<sup>th</sup> Cong. (2022).

<sup>275</sup> See, e.g., H.R. 8152 ("A covered entity or a service provider may not collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability."); S. 2499 (buttressing existing federal civil rights laws, enlisting the support of the FTC to refer possible violations to other agencies, and ordering the FTC to conduct a study of algorithmic discrimination); S. 3195 (prohibiting the use of covered data to facilitate discriminatory advertising or eligibility determinations in the areas of housing, employment, credit, and education opportunity).

<sup>276</sup> Fourth Amendment Is Not For Sale Act, S. 1265, 117<sup>th</sup> Cong. (2021).

<sup>277</sup> DELETE Act, S. 3627, 117<sup>th</sup> Cong. (2022).

In the digital era, a great deal of information sharing has become unavoidable for the average person, a significant change in factual context that matches the same historical pattern of unavoidability that triggered much of the existing body of U.S. privacy law. Policymakers historically responded to similar factual contexts by adopting laws focused on restoring avoidability, but in many circumstances, avoidability simply can no longer be restored. This explains policymakers' current struggle to define the appropriate scope and goals of legislation to adequately address the same goals that have been addressed in past privacy protections for information shared unavoidably.