Cleveland State Law Review

Volume 66 | Issue 3 Article

5-15-2018

# Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)

John A. Rothchild
*Wayne State University Law School*

# AGAINST NOTICE AND CHOICE: THE MANIFEST FAILURE OF THE PROCEDURALIST PARADIGM TO PROTECT PRIVACY ONLINE (OR ANYWHERE ELSE)

JOHN A. ROTHCHILD*

ABSTRACT

Notice and choice are the foundational principles underlying the regulation of privacy in online transactions and in most other situations in which individuals interact with the government and commercial interests. These principles mean that before collecting personally identifiable information ("PII") from an individual, the collector must provide the individual with a disclosure (notice) of what PII it proposes to collect and how it proposes to use that information. That knowledge enables the individual to make a rational decision (choice) about whether to allow that collection of information, generally by declining to enter into the transaction or, in some situations, by denying consent to collect the PII.

This Article argues that the notice-and-choice paradigm is fundamentally flawed, cannot be fixed, and should be replaced with a system that places substantive limitations on the collection and use of PII for commercial purposes.

Each of us who engages with commercial websites, mobile computing devices, or everyday devices that are connected to the Internet receives these notices many times every day. The notices are typically conveyed in the text of a privacy policy that can be accessed by clicking on a hyperlink at the bottom of a web page, tapping on a link of a mobile app's page on a distribution platform, or paying close attention when installing an Internet of Things device. And the great majority of us, just as many times each day, ignore these privacy notices and submit to whatever collection of PII may result.

Why do presumably rational users of the Internet fail to take advantage of this wealth of disclosure information, which is only a click away? Our behavior is easily explained by the concept of "rational inattention." The human condition of bounded rationality makes it infeasible for us to take in and process all the information that is contained in the privacy notices that surround us. Even if we were able to process these notices, it would do us no good because, as demonstrated by an empirical study included in this Article, the uniformity among these privacy policies means that we cannot choose among more- and less-protective policies: we can only choose to engage with the online world, making our PII available for uses that we cannot understand or evaluate, or become hermits in self-exile from the online world.

The alternative this Article proposes is to discard our faith in the proceduralist approach of notice-and-choice and develop substantive rules that will truly protect the privacy of individuals in their online interactions, rather than settling for the simulacrum of privacy protection that the present system offers.

---

* Associate Professor of Law, Wayne State University Law School. I gratefully acknowledge the contributions to this Article from my outstanding research assistants: David Bergh, Alex F. Bowman, Nhan Ho, and Casey Monahan. 

CONTENTS

## I. INTRODUCTION

"Notice" and "choice" are foundational elements of the reigning paradigm for reconciling individual interests in information privacy with the interests of commercial and government entities in processing personally identifiable information ("PII").[1] The paradigm requires an information collector to disclose to an individual what personal information it proposes to collect from her and how it proposes to use that information ("notice"), thereby affording the individual an opportunity to prevent the collection of her PII by denying consent or by declining to enter into the transaction

[1] "Personally identifiable information" ("PII") is the standard term used in discussions of privacy in legal contexts. Definitions of the term vary somewhat. The Government Accountability Office has defined PII as:

> (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-536, ALTERNATIVES EXIST FOR ENHANCING PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION 1 n.1 (2008). This definition will suffice for present purposes.

("choice").[2] In this Article, I argue that notice-and-choice is a fatally flawed approach to protecting the private information that is generated through the use of the various communications facilities that depend on the Internet. It is time to recognize the failure of the proceduralist paradigm and move to a new approach that includes substantive rules regulating the conduct of would-be users of our private information.

The Internet-dependent communications facilities include commercial websites, mobile computing devices, and the Internet of Things ("IoT"). (I will sometimes refer to the information transmitted using these communications facilities as Internet-enabled data flows.) Notice-and-choice did not work well starting with the earliest commercial interactions making use of the Internet, namely through sites on the World Wide Web. It has worked progressively less well with the rise of social media platforms, which has brought about a dramatic leap in the amount of private information our online activity exposes,[3] and as we have left our desktop computers behind in preference for mobile devices.[4] The coming age of the IoT[5] offers an occasion to assess the suitability of notice-and-choice in that context as well.

Criticisms of notice-and-choice in the online context abound. The critics generally do not reject the paradigm,[6] but only its implementations, calling for shorter and more

[2] Thomas B. Norton, Note, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 184 (2016).

[3] According to one tabulation, on average people spend nearly two hours a day using social media, representing thirty percent of their online time. Evan Asano, *How Much Time Do People Spend on Social Media? [Infographic]*, SOCIALMEDIATODAY (Jan. 4, 2017), http://www.socialmediatoday.com/marketing/how-much-time-do-people-spend-social-media-infographic. This is up from fifteen minutes a day in 2012. *See* Jason Mander, *Social Media Captures 30% of Online Time*, GLOBALWEBINDEX (June 8, 2016), http://blog.globalwebindex.net/chart-of-the-day/social-media-captures-30-of-online-time/.

[4] Starting in 2014, with the gap continuing to increase since then, mobile devices surpassed desktop computers in terms of number of users globally and hours of usage each day. Dave Chaffey, *Mobile Marketing Statistics Compilation*, SMART INSIGHTS (Mar. 1, 2017), http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/.

[5] According to one report, in 2017 the IoT consisted of 20 billion devices. Peter Brown, *20 Billion Connected Internet of Things Devices in 2017, IHS Markit Says*, ELECTRONICS360 (Jan. 25, 2017), http://electronics360.globalspec.com/article/8032/20-billion-connected-internet-of-things-devices-in-2017-ihs-markit-says. Projections of growth in the number of connected devices vary widely, but all expect dramatic increases. *IoT Market Forecasts*, POSTSCAPES, https://www.postscapes.com/internet-of-things-market-size/ (last visited Jan. 23, 2018).

[6] An exception is Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 341 (Jane K. Winn ed., 2006) (proposing a set of "Consumer Privacy Protection Principles" as an alternative to the Fair Information Practice Principles).

readable privacy policies,[7] notice that is more prominently presented to the data subject[8] or is rethought,[9] and other refinements.[10]

These prescriptions are inadequate because the diagnosis is wrong. The problems with notice-and-choice are not fixable because they are inherent to its fundamental structure. As I explain in what follows: First, the notice-and-choice paradigm assumes that data subjects behave rationally, and yet requires them to devote an irrational amount of effort to reading and evaluating privacy policies in order to determine whether to engage with a particular entity or product. Second, the "notice" element of notice-and-choice, as presently implemented, is plainly inadequate under accepted standards that apply in the related contexts of contracting and consumer protection; any effort to bring about adequate presentation of privacy notices is doomed to failure due to the limits of human cognition. Third, the uniformity of privacy policies means that the "choice" element of notice-and-choice is illusory. Fourth, notice-and-choice amounts to blanket consent, which is generally disfavored in privacy contexts. Fifth, the commanding role that third parties play in the dissemination and use of private information collected from Internet-enabled data flows makes it impossible for a privacy notice to specify what an individual needs to know to make an informed choice about the disposition of her private information. And sixth, notice-and-choice cannot be implemented with respect to IoT devices that collect personal information from persons other than the owner or deployer of the device.

If notice-and-choice is broken and cannot be fixed, what is the alternative? I argue that it is necessary to jettison the proceduralist approach of notice-and-choice and adopt substantive limitations on the collection and use of PII through Internet-enabled data flows. Notice-and-choice is a procedural rule in that, as long as it follows the prescribed procedures, tendering notice and obtaining consent, a data processor may collect any private information and use it for any purpose. A substantive privacy rule, on the other hand, deems certain conduct impermissible even with notice and consent.

---

[7] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 64 (2012) [hereinafter FTC, PROTECTING CONSUMER PRIVACY], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."); Patrick Gage Kelley et al., *A "Nutrition Label" for Privacy*, *in* PROCEEDINGS OF THE FIFTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 4 (2009) (proposing redesign of privacy notices along the lines of nutrition labeling); Marcus Moretti & Michael Naughton, *Why Privacy Policies Are So Inscrutable*, ATLANTIC (Sept. 5, 2014), http://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/ (advocating a switch to "plain language privacy policies that make consumers want to read").

[8] *See, e.g.*, KAMALA D. HARRIS, ATT'Y GEN., CAL. DEP'T OF JUSTICE, MAKING YOUR PRIVACY POLICIES PUBLIC 9 (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf ("Use a conspicuous link on your homepage containing the word 'privacy.'").

[9] *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1030 (2012) (advocating use of "visceral notice").

[10] *See* Paula J. Bruening & Heather M. Patterson, *A Context-Driven Rethink of the Fair Information Practice Principles* (Sept. 23, 2016), http://dx.doi.org/10.2139/ssrn.2843315 (advocating injection of contextual considerations into the fair information practice principles).

Doctrinally, substantive privacy rules can be premised on theories of unfairness and unconscionability. In multiple cases, the Federal Trade Commission ("FTC") has found privacy-invading practices to be "unfair" acts in violation of the FTC Act.[11] In the closely related context of information security, the FTC routinely finds the failure to maintain reasonable security practices to be unfair.[12] Common law and statutory concepts of unconscionability also are applicable.[13]

What sorts of substantive privacy rules should we apply to consumer-facing, Internet-enabled commercial data flows? That is a subject for another inquiry, but I suggest one: A company should be forbidden to condition provision of a good or service to a consumer on the consumer's consent to collection or use of private information that is not required for provision of the good or service.

This Article proceeds as follows. In Section II, I discuss the four waves of computing technology that have given rise to different contexts relevant to the principles of notice and choice. In Section III, I analyze the role that notice-and-choice plays in several of the more influential formulations of a widely recognized set of privacy principles, illuminating their similarities and differences. I then do the same with implementations of the principles in positive law and in self-regulatory schemes. In Section IV, I explain why notice-and-choice has always been, and in the future promises more and more to be, a failure if the goal is to give consumers the ability to control the collection and use of their PII. In Section V, I sketch out a way forward: eschew sole reliance on the procedural paradigm of notice-and-choice and develop substantive rules that will actually promote the privacy interests of real people functioning in the real world rather than merely providing a soothing but ultimately ineffectual system of notice-and-choice. In Section VI, I briefly conclude.

## II. THE TECHNOLOGY AND METHODOLOGY OF COLLECTING AND USING PRIVATE INFORMATION EXPOSED THROUGH INTERNET-ENABLED DATA FLOWS

To understand the information privacy issues that arise from Internet-enabled data flows, we need to understand the technology used to gather and process the private information contained in these data flows. For purposes of this analysis, the technology can be classified into four phases. These phases have arisen at successive points in time, but they are cumulative rather than consecutive. That is, technologies introduced in the earlier phases have never entirely died out, but continue to be used in the later phases.

### *A. Collection and Storage of Private Data*

#### 1. Databases on Mainframe Computers (Early 1950s to Present)

The earliest computing technology that gave rise to privacy issues was automated data processing using mainframe computers.[14] The use of computers to process commercial data first arose in the late 1940s and early 1950s as demobilization after

[11] *Infra* Section V.B.1.a.

[12] *Infra* Section V.B.1.b.

[13] *Infra* Section V.B.2.

[14] The meaning of the term "mainframe" has evolved over the years with developments in computing technology. For present purposes, it may be defined as a "large computer used for commercial data processing and other large-scale operations." THE HUTCHINSON DICTIONARY OF COMPUTING AND THE INTERNET 344 (2005).

World War II resulted in a tremendous boom in commercial transactions. The federal government was an early adopter and thereby helped to spread the use of electronic data processing.[15] The first few UNIVAC computers were sold in the early 1950s to the United States Census Bureau, the military, and the Atomic Energy Commission.[16] Starting in 1954, these machines were sold to large corporations such as General Electric, Metropolitan Life, and Consolidated Edison.[17] Some of the applications of these machines, such as General Electric's use of them to produce payroll checks for its employees,[18] began to implicate privacy interests.

During the 1960s and early 1970s, commentators drew public attention to the looming risks to privacy that they perceived from the growing use of computers to store and manipulate personal information.[19] One particular catalyst was a 1965 proposal that the federal government create a "national data center" that would consolidate computerized records then scattered among twenty federal agencies.[20] The proposal gave rise to congressional hearings and outrage in the popular press over the privacy implications of such a centralized database. Ultimately, the privacy issues scuttled the proposal and led to the enactment of the Privacy Act of 1974.[21]

Alarm over the privacy implications of automated data processing on a large scale persuaded the Secretary of Health, Education, and Welfare to convene an advisory committee charged with producing a report on the subject.[22] At the time, the government was seen as posing the principal threat to privacy, and not much concern existed about the role of private companies as a source of privacy invasions.[23] For

---

[15] *See* SHANE GREENSTEIN, HOW THE INTERNET BECAME COMMERCIAL 70 (2015) (describing early purchases of computer technology by NASA, the Department of Defense, and other federal government agencies).

[16] *UNIVAC: UNIVersal Automatic Computer*, HIST. COMPUTING PROJECT, https://www.thocp.net/hardware/univac.htm (last updated Mar. 14, 2013).

[17] *See* PAUL E. CERUZZI, A HISTORY OF MODERN COMPUTING 28 (2d ed. 2003).

[18] *Id.* at 32–33.

[19] *See* MYRON BRENTON, THE PRIVACY INVADERS 14 (1964) (noting privacy challenges resulting from "the growing use of giant computer systems to house all the file information"); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 30 (1971) (warning of the risk that "an ingenious wiretapper" might gain unauthorized access to computerized information in transit); VANCE PACKARD, THE NAKED SOCIETY 35 (Pocket Cardinal ed. 1965) ("Americans should be uneasy about the amount of information the federal government is starting to file on its citizens in its blinking memory banks."). For a canvass of the concerns raised about the privacy implications of computers beginning in the early 1960s, see ALAN F. WESTIN, PRIVACY AND FREEDOM 298–321 (1st ed. 1967).

[20] Rebecca S. Kraus, *Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants*, 5 J. PRIVACY & CONFIDENTIALITY 1 (2013).

[21] *Id.*

[22] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 7–8 (1973) [hereinafter HEW REPORT].

[23] *See* WILLIS H. WARE, RAND AND THE INFORMATION EVOLUTION 155 (2008), https://www.rand.org/pubs/corporate_pubs/CP537.html ("[T]he government was seen as 'the privacy problem' in the 1970s. . . ."). Ware served as the chair of the committee that produced the 1973 HEW Report. *Id.* at 154.

example, the report expressed concern that the National Driver Register, a computer database maintained by the National Highway Traffic Safety Administration in Washington, D.C., could be mined in a "dragnet" operation, that is, a "systematic screening of all members of a population in order to discover a few members with specified characteristics."[24] The report also discusses the "social control capabilities" of a federally managed health information system that maintained medical records on 14,000 Native Americans living on a particular reservation in the southwest United States.[25] On the immediate horizon, another matter for concern was the FBI's National Crime Information Center, "a computerized clearinghouse of information about wanted persons, stolen property, and criminal history records."[26]

In this pre-Internet era, information about us was collected from tabulation of our everyday activities and was assembled into ever-more-comprehensive databases. Personal information continues to be collected from offline sources.[27] Credit card companies compile information about every transaction in which a consumer uses the card. Consumer credit bureaus record information about payment of our debts and other information that is used to determine our credit-worthiness.[28] Stores keep information about their walk-in and telephone customers.[29] Magazine publishers retain information about their subscribers.[30] Other offline sources of PII include telephone companies, automobile dealers, warranty registrations, and contest entries.[31] In a

[24] HEW REPORT, *supra* note 22, at 15 n.2. The National Driver Register, established by federal law in 1961, was a centralized database of persons whose application for a driver's license had been denied or whose license had been revoked. *Id.* at 15. Its ostensible purpose was to prevent such persons from evading the denial of a license in one state by applying for one in another state; without a centralized registry, the second state would not know about the first state's action. *Id.* The data-management technology was primitive by today's standards: a state DMV would update the database by using postal mail to send magnetic tape, computer punch cards, or typewritten forms to the maintainer of the database in Washington, D.C., and queries of the system by DMVs would likewise be answered by postal mail. *Id.* at 202–21. The NDR still exists and continues to operate, with upgraded technology. NHTSA, *National Driver Register*, U.S. DEP'T OF TRANSP., https://www.nhtsa.gov/research-data/national-driver-register-ndr (last visited Jan. 24, 2018).

[25] HEW REPORT, *supra* note 22, at 24–27.

[26] *Id.* at 17.

[27] *See* Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK (May 30, 2016), http://www.newsweek.com/secretive-world-selling-data-about-you-464789.

[28] *Id.*

[29] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 28 (2014) [hereinafter FTC, DATA BROKERS], https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[30] *Id.* at 13.

[31] *Id.* at 13–14.

process sometimes called "onboarding," data brokers combine offline with online information,[32] as do online platforms like Google and Facebook.[33]

2. Enter the Internet (1995 to Present)

The collection of PII entered a new phase with the inception of the commercial Internet in 1995.[34] Interactions between consumers and businesses via the World Wide Web generated new types of PII that were available to be harvested using new technologies. As retail commerce increasingly shifts from brick-and-mortar outlets to online shopping, more and more of the PII generated from our commercial interactions can be acquired and centralized through these techniques.[35]

Some of the information collection is transparent to the user. For example, every time you make an online purchase, you transmit the information that is needed to complete the transaction: at a minimum, your identity and the products or services that you have purchased. If the item purchased is a physical one that must be delivered, you will also hand over your mailing address. Even if no physical delivery is involved (such as music or books in electronic formats), you usually will pay with a credit card, revealing your identity.

Other information is swept up from online activity in ways that are not transparent to the typical user. When you access a website, the site owner may collect information such as each web page that you view, how much time you spend on each page,

---

[32] *Id.* at 27.

[33] *See* Heather Kelly, *Google Expands Ad Tracking in the Real World*, CNN (May 23, 2017), http://money.cnn.com/2017/05/23/technology/google-ads-real-world/index.html ("A new Google [] feature can tell when someone who clicked on an ad in search results made a credit or debit card purchase at a corresponding physical store."). For a discussion of how onboarding is accomplished, see Michelle Geronimo, Note, *Online Browsing: Can, Should, and May Companies Combine Online and Offline Data to Learn About You?*, 9 HASTINGS SCI. & TECH. L.J. 211, 212–19 (2017).

[34] Although limited commercial activity was conducted on the Internet before 1995, that year is a plausible one for the start of the commercial Internet because it was when the National Science Foundation decommissioned the NSFNet and relinquished its role in governance of the network, thereby eliminating the NSFNet's Acceptable Use Policy, which had prohibited commercial use. JANET ABBATE, INVENTING THE INTERNET 199 (1999) (discussing how privatization of the Internet in 1995 allowed it to be used for commercial purposes); Janet Abbate, *Privatizing the Internet: Competing Visions and Chaotic Events, 1987–1995*, IEEE ANNALS HIST. COMPUTING, Jan.–Mar. 2010, at 14–15 (discussing the NSF's Acceptable Use Policy); *see also A Brief History of NSF and the Internet*, NAT'L SCI. FOUND., https://www.nsf.gov/news/special_reports/cyber/internet.jsp (last visited Mar. 7, 2018). The year 1995 was also when Netscape first released its browser commercially and when both Amazon.com and eBay began their operations. *See* GREENSTEIN, *supra* note 15, at 116 (explaining that commercial versions of Netscape first became available in 1995); *id*. at 220 (noting that Yahoo!, eBay, Amazon, and other online businesses started in 1994–95).

[35] The proportion of all retail activity that is conducted through ecommerce, according to the Census Bureau's definition of the term, has risen from 0.6% in the fourth quarter of 1999 to 9.1% in the fourth quarter of 2017. U.S. CENSUS BUREAU, QUARTERLY RETAIL E-COMMERCE SALES (Feb. 16, 2018), https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf (Fourth Quarter of 2017); U.S. DEP'T OF COMMERCE, RETAIL E-COMMERCE SALES FOR THE FOURTH QUARTER 1999 REACH $5.3 BILLION, CENSUS BUREAU REPORTS (Mar. 2, 2000), https://www2.census.gov/retail/releases/historical/ecomm/99q4.pdf (Fourth Quarter of 1999).

products that you examine but do not buy, and the web page that you were viewing before arriving at the website.[36] Google, through its search engine and other online offerings, "logs personal identifying information, browsing habits, search queries, responsiveness to ads, demographic information, declared preferences and other information about each consumer that uses its products."[37]

Online businesses have deployed a variety of technologies for collecting and manipulating PII. The most basic of these is the cookie: an identifying tag that is placed on the user's computer through an interaction between her browser and the website's server, which allows the site visitor to be recognized on subsequent visits.[38] Cookies and other identification techniques[39] allow much of a user's clickstream data, generated through visits to many websites, to be assembled into a single dossier that is associated with that individual.[40] Online advertising networks, which place cookies on a consumer's computer through their arrangements with millions of websites, allow information from a user's visits to multiple websites to be assembled into a single dossier.[41]

Consolidation within the industry offers additional avenues for aggregating data. In 2007, Google acquired DoubleClick, a leading advertising network, but pledged to keep the personal information it obtained through DoubleClick cookies separate from

---

[36] *See* Abdelmounaam Rezgui et al., *Privacy on the Web: Facts, Challenges, and Solutions*, IEEE SECURITY & PRIVACY, Nov.–Dec. 2003, at 43.

[37] *In re* Google, Inc. Privacy Policy Litig., No. 5:12-CV-001382-PSG, 2015 WL 4317479, at *2 (N.D. Cal. July 15, 2015).

[38] Erica M. Scott, Comment, *Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a Trans-Atlantic Browser-Based Opt-In for Behavioral Tracking the Right Solution?*, 26 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 285, 289–91 (2013).

[39] Other techniques include "web bugs" (generally referred to by their deployers using the less-sinister-sounding terms "web beacons" or "pixel tags"), which transmit information when a user accesses a tagged web page or opens an email message; flash cookies, which can be used to regenerate deleted cookies; spyware, software that is surreptitiously downloaded to a consumer's computer and secretly gathers and transmits information derived from the consumer's use of the computer; and unique device identifiers, which can reside in either hardware or software. *Means and Methods of Web Tracking: Its Effects on Privacy and Ways to Avoid Getting Tracked*, INFOSEC INST. (July 23, 2013), http://resources.infosecinstitute.com/means-and-methods-of-web-tracking-its-effects-on-privacy-and-ways-to-avoid-getting-tracked/#gref. Thus, a user cannot thwart tracking by the simple expedient of blocking or deleting cookies. *See id.*

[40] *See* FED. TRADE COMM'N, ONLINE PROFILING 4, 12 (2000) [hereinafter FTC, ONLINE PROFILING], https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf (describing how previously anonymous information can become personally identified); Scott, *supra* note 38, at 291–92 (describing how non-PII clickstream data may become identified with an individual by aggregating multiple sources of information); Jessica Su et al., *De-anonymizing Web Browsing Data with Social Networks*, PROC. 26TH INT'L CONF. WORLD WIDE WEB 1261 (2017) (showing that anonymous browsing history can be de-anonymized and linked to the user's social media accounts).

[41] FTC, ONLINE PROFILING, *supra* note 40, at 2–8 (discussing the role of network advertising companies).

that which it got through its other online properties. In 2016, it abandoned that pledge and began combining the two sets of information, allowing it to better identify users of the Web and track them as they engage in various online activities.[42]

In addition to these interactions with online sellers of goods and services, we generate information about ourselves through our activity on social media. We post information about our likes and dislikes, enter into discussions with other social media users through postings and comments, state political positions, and more. Facebook keeps track of everything we do on its site and uses what it gathers to enable marketers to target advertisements at us.[43] While some social media sites place restrictions on the ability of data aggregators to collect information from their sites using automated methods, others do not.[44] This information, though not generated through commercial activity, is commercially valuable because it reveals preferences that can be used as an input into targeted marketing. Most Facebook users probably are unaware that by clicking on "Like" buttons they may be providing Facebook with a more accurate assessment of their personality than those made by their (real-life) friends and even family members.[45]

3. Mobile Apps (2007 to Date)

Computers that are small enough to be carried in a pocket, capable of connecting to the Internet wirelessly, and able to determine their geographical location first became widely available in 2007 as the Apple iPhone.[46] Tablet computers first gained widespread popularity with the introduction of Apple's iPad in 2010.[47] From 2011 to 2018, the percentage of adults in the United States who own a smartphone increased from 35% to 77%.[48] Software applications that run on mobile devices, called apps,

---

[42] Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking*, PROPUBLICA (Oct. 21, 2016), https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking.

[43] *See* Adrienne LaFrance, *Facebook Is Expanding the Way It Tracks You and Your Data*, ATLANTIC (June 12, 2014), https://www.theatlantic.com/technology/archive/2014/06/facebook-is-expanding-the-way-it-tracks-you-and-your-data/372641/; Olivia Solon, *How Much Data Did Facebook Have on One Man? 1,200 Pages of Data in 57 Categories*, WIRED (Dec. 28, 2012), http://www.wired.co.uk/article/privacy-versus-facebook.

[44] FTC, DATA BROKERS, *supra* note 29, at 13.

[45] Wu Youyou et al., *Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans*, 112 PROC. NAT'L ACAD. SCI. 1036 (2015) (reporting results of a study showing that a computer model needed 70 Likes to judge personality more accurately than a friend and 150 Likes to judge more accurately than a family member).

[46] The evolution of the smartphone from IBM's Simon Personal Computer, introduced in 1992, to the iPhone in 2007 is discussed in ANINDYA GHOSE, TAP: UNLOCKING THE MOBILE ECONOMY 21–22 (2017).

[47] Earlier offerings of tablet computers were less successful. *See* David Nield, *15 Memorable Milestones in Tablet History*, TECHRADAR (July 5, 2016), http://www.techradar.com/news/mobile-computing/10-memorable-milestones-in-tablet-history-924916.

[48] *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.

have been available from the Apple App Store and Google Play Store (for Android) since 2008.[49]

Paralleling the rise in smartphone ownership is a rise in the proportion of electronic commerce resulting from the use of smartphones. In 2014, mobile commerce was 11.6% of total ecommerce, and one analysis expects the proportion to rise to 45% in 2020.[50]

Users of mobile phones can be tracked in several ways. Each smartphone has a unique identifier associated with it. Data analytics companies are able to link the phone's identifier with the owner's identity and then combine data that the user generates by using the phone with data about him from other sources.[51]

In addition to the clickstream information, mobile devices can determine and make available the user's ever-changing geographical location. The user's location at the time she accesses a website or uses an app can reveal highly sensitive information. When does she arrive at and leave her workplace? How much time does she spend in bars? Did she visit an adult novelty shop?[52] Advertising platforms are able to target advertisements at the user of a mobile phone based on the user's current or historical location.[53]

---

[49] John Markoff & Laura M. Holson, *Apple's Latest Opens a Developers' Playground*, N.Y. TIMES (July 10, 2008), http://www.nytimes.com/2008/07/10/technology/personaltech/10apps.html. Google Play was originally called Android Market. Melissa Perenson, *Google Launches Android Market*, PCWORLD (Oct. 22, 2008), http://www.pcworld.com/article/152613/google_android_ships.html.

[50] Andrew Meola, *The Rise of M-Commerce: Mobile Shopping Stats & Trends*, BUS. INSIDER (Dec. 21, 2016), http://www.businessinsider.com/mobile-commerce-shopping-trends-stats-2016-10.

[51] Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1254 (11th Cir. 2015) (discussing an analytics company that can "link an Android ID to a particular person by compiling information about that individual from other websites, applications, and sources").

[52] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."). In that concurrence, Justice Sotomayor quotes from People v. Weaver, 909 N.E.2d 1195, 1199 (2009) as follows:

> Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.

*Jones*, 565 U.S. at 415.

[53] *See* United States v. InMobi Pte Ltd., No. 3:16-cv-3474 (N.D. Cal. June 27, 2016) (describing the technology behind "geo-targeting" of advertisements to mobile phones in a case where the FTC charged that the advertising company misrepresented that it would geo-target only if the user had location services turned on, when in fact it also did so by using Wi-Fi location information even when location services was turned off).

Internet connectivity on mobile devices allows an advertising technique known as "geofencing" or "geo-targeting."[54] The advertiser monitors a person's location using the device's geolocation technology (using GPS, proximity of Wi-Fi access points, and other techniques) and then sends an advertisement to the device based on the location. A digital advertising company allegedly used geofencing to send anti-abortion messages to the smartphones of users who it determined were located at a reproductive health facility.[55] The Massachusetts Attorney General considered this an unfair or deceptive act in violation of the state consumer protection law and obtained the company's agreement not to engage in geofencing of medical facilities in Massachusetts.[56]

4. The Internet of Things (2011[57] to Date)

As I use the term, the Internet of Things ("IoT") consists of consumer-facing devices that are connected to the Internet but historically were not so connected.[58] This definition excludes computers of all sorts, which have commonly been connected to the Internet for the past decade or two, a wide range of connected sensors with industrial applications,[59] and perhaps smartphones as well. The term itself is said to derive from a presentation that Kevin Ashton, a British technology entrepreneur, made

[54] *See* Kathleen Kusek, *5 Ways Facebook Geo-Targeting Will Change Your Life*, FORBES (Oct. 11, 2014), https://www.forbes.com/sites/kathleenkusek/2014/10/11/5-ways-facebook-geo-targeting-will-change-your-life/#6a77e92b17c4.

[55] Hiawatha Bray, *Sending Anti-Abortion Ads by Phone Is Creepy, but Not Illegal*, BOS. GLOBE (Apr. 5, 2017), https://www.bostonglobe.com/business/2017/04/05/sending-anti-abortion-ads-phone-creepy-but-not-illegal/Aa5wZeYCd4NUOO65n8CgIL/story.html.

[56] Assurance of Discontinuance Pursuant to G.L. 93A, § 5, *In re* Copley Advert., LLC, No. 1784CV01033 (Mass. Super. Ct. Apr. 4, 2017); Press Release, AG Reaches Settlement with Advertising Company Prohibiting "Geofencing" Around Massachusetts Healthcare Facilities (Apr. 4, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html.

[57] I use 2011 as the starting date to reflect the fact that Nest Labs introduced its Nest Learning Thermostat, the first widely popular IoT device, in that year. *Nest Labs Introduces World's First Learning Thermostat*, NEST (Oct. 25, 2011), https://nest.com/press/nest-labs-introduces-worlds-first-learning-thermostat/. In 2014, Google purchased Nest Labs for $3.2 billion. Nathan Ingraham, *Google Purchases Nest for $3.2 Billion*, VERGE (Jan. 13, 2014), https://www.theverge.com/2014/1/13/5305282/google-purchases-nest-for-3-2-billion.

[58] There is no generally accepted definition of the term. For a bewildering array of definitions, see *Best Internet of Things Definition*, POSTSCAPES (Nov. 14, 2015), http://postscapes.com/internet-of-things-definition.

[59] Industrial applications include "[j]et engines and delivery trucks [that] can now be outfitted with sensors that monitor hundreds of data points and send automatic alerts when maintenance is needed." EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 5–6 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

in 1999.[60] The first devices that are now acknowledged to have belonged to the proto-IoT are dated to the 1980s and 1990s.[61]

The past few years have seen a remarkable proliferation of IoT devices. At the 2015 Consumer Electronics Show, some 900 exhibitors showed off new IoT devices.[62] Many of these, like an in-refrigerator egg counter or a connected diaper, may never find a wide market.[63] Yet others will doubtless gain traction in the marketplace.

Many IoT devices are designed to be placed in the home, some of them in close proximity to our most intimate activities. These include light bulbs,[64] kitchen and laundry appliances,[65] kitchen scales,[66] water leak sensors,[67] smoke and carbon monoxide detectors,[68] doorbells with video,[69] baby monitors,[70] home thermostats,[71]

---

[60] *See* Kevin Ashton, *That "Internet of Things" Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/view?4986. Other terms that have been used for the same or similar concepts include ubiquitous computing, pervasive computing, the web of things, the physical web, home automation, smart-X (e.g., smart homes, smart cities, smart grid), and connected-X (e.g., connected cars). *See* Maria R. Ebling, *Pervasive Computing and the Internet of Things*, 15 IEEE PERVASIVE COMPUTING 2 (2016).

[61] Candidates for the "first" IoT device include: a Coca-Cola vending machine at the Carnegie Mellon University Computer Science Department that, in 1982, was connected to the university's network so that users of the machine could check from their desks whether it was empty and whether the bottles were cold, *The "Only" Coke Machine on the Internet*, CARNEGIE MELLON U., http://www.cs.cmu.edu/~coke/history_long.txt (last visited Mar. 7, 2018); a toaster that could be controlled via the Internet in 1990, Peter Waterhouse, *Internet of Everything: Connecting Things Is Just Step One*, INFORMATIONWEEK (Dec. 9, 2013), http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-everything-connecting-things-is-just-step-one/d/d-id/1112958; and a coffee pot at a computer research laboratory at Cambridge University in 1991 that could be viewed via a webcam, *see* Quentin Stafford-Fraser, *The Story of the Trojan Room Coffee Pot*, U. CAMBRIDGE, http://www.cl.cam.ac.uk/coffee/qsf/timeline.html (last visited Mar. 7, 2018).

[62] Andrea Chang, *At CES, "Internet of Things" Showcases the Connected Life*, L.A. TIMES (Jan. 6, 2015), http://www.latimes.com/business/la-fi-ces-internet-things-20150106-story.html.

[63] David Pogue, *The Good, the Bad and the Weirdest "Internet of Things" Things*, SCI. AM. (July 1, 2016), https://www.scientificamerican.com/article/pogue-the-good-the-bad-and-the-weirdest-internet-of-things-things/.

[64] *Hue Personal Wireless Lighting*, PHILIPS, http://www2.meethue.com/en-us/ (last visited Mar. 7, 2018).

[65] GE APPLIANCES, http://www.geappliances.com/ge/connected-appliances/ (last visited Mar. 7, 2018).

[66] DROP, https://getdrop.com/ (last visited Mar. 7, 2018).

[67] LA CROSSE TECHNOLOGY, http://www.lacrossetechnology.com/remote-water-leak-detector/ (last visited Mar. 7, 2018).

[68] ONELINK, https://onelink.firstalert.com/ (last visited Mar. 7, 2018).

[69] RING, https://ring.com/ (last visited Mar. 7, 2018).

[70] IBABY, https://ibabylabs.com/ (last visited Mar. 7, 2018).

[71] NEST THERMOSTAT, https://nest.com/ (last visited Mar. 7, 2018).

bathroom scales,[72] home security systems,[73] home security cameras,[74] door locks,[75] toothbrushes,[76] window shades and blinds,[77] garage door openers,[78] and many other items. Adoption of these devices is likely to receive a boost due to the popularity of the Amazon Echo and Google Home, which one can use to control many of these devices by speaking voice commands.[79]

Many of these devices (such as home security cameras and baby monitors) are always on—taking in data from the environment continuously and handling it in ways that will be largely unknown to most who invite the technology into their homes. For example, voice-operated assistants for the home, dominated by the Amazon Echo (powered by the Alexa voice assistant) and Google Home, are always listening for the keyword that "wakes" them.[80] One's commands to the device are transmitted to a server somewhere in the cloud, where they are stored and processed, thereby enabling the device to respond.[81] One can subsequently delete the recordings by accessing his account on the Web, but "it's unclear whether the data survives on servers after you delete it from the queue in [his] account."[82]

The quantity of data collected by IoT devices is astounding, far outstripping the amount of data that people create volitionally through emails, online postings,

---

[72] GARMIN INDEX SMART SCALE, https://buy.garmin.com/en-US/US/p/530464 (last visited Mar. 7, 2018).

[73] ADT, https://www.adt.com/wireless-security (last visited Mar. 7, 2018).

[74] D-LINK, http://us.dlink.com/home-solutions/wifi-camera/ (last visited Mar. 7, 2018).

[75] AUGUST, http://august.com/products/august-smart-lock/ (last visited Mar. 7, 2018).

[76] ORAL-B, https://oralb.com/en-us/products/genius-8000-electric-toothbrush-with-bluetooth (last visited Mar. 7, 2018).

[77] SERENA, https://www.serenashades.com/serenaadvantage/connected-home (last visited Mar. 7, 2018).

[78] LIFTMASTER, https://www.liftmaster.com/for-homes/myq-connected-home (last visited Mar. 7, 2018).

[79] Hiawatha Bray, *Do Alexa and Other Such Devices Mean the End of Privacy?*, BOS. GLOBE (Jan. 12, 2017), https://www.bostonglobe.com/business/2017/01/11/alexa-and-other-internet-things-devices-mean-end-privacy/ry8wyKTY48KVOSvqoZSe6M/story.html (discussing the privacy implications of using the voice-controlled Echo "to switch on your lights, unlock the front door, or warm up the car"). Amazon sold over ten million Echo devices in the two years after it was introduced. Google has sold about a third as many Google Home devices. Brian Deagon, *Amazon Echo Keeps Big Lead over Google Home in Digital Assistants*, INV. BUS. DAILY (May 8, 2017), http://www.investors.com/news/technology/amazon-echo-maintains-big-lead-over-google-home-in-digital-assistants/.

[80] Stephen Harrison, *Don't Call It "Siri": Why the Wake Word Should Be "Computer"*, SALON (Nov. 26, 2017), https://www.salon.com/2017/11/26/dont-call-it-siri-why-the-wake-word-should-be-computer/.

[81] Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to That Data?*, WIRED (Dec. 5, 2016), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/.

[82] *Id.*

photographs, videos, music, and all other media.[83] Yet, because IoT devices are, by (my) definition, ones that have traditionally not been connected to a network, the fact that these devices are siphoning up personal information may be less obvious than is the case with computers.

Data collected by IoT devices travels via the public Internet, opening an avenue for privacy invasions through unauthorized access to the data. There have been several well-publicized incidents of privacy invasions tied to Internet-connected cameras. In 2014, the FTC brought an enforcement action against TRENDnet, Inc., a manufacturer of IP-connected cameras intended for use in homes and by small businesses. In its complaint, the FTC alleged that from 2010 to 2012, the respondent's software contained a flaw that caused the camera user's security settings to be ignored, allowing hackers to gain access to the video feed of users who had selected a setting that was supposed to make the feed private and accessible only by entering login credentials.[84] As a result, hackers posted links online that allowed anyone to monitor the live feeds from nearly 700 of the cameras.[85]

Another webcam privacy issue involves surreptitious, remote activation of a connected camera. A malicious hacker can activate the camera incorporated into a laptop computer by tricking the computer user into downloading software called a "remote access Trojan," using techniques that are standard in the hacking community.[86] Once installed, the software allows the hacker to activate the camera remotely—in some cases while preventing the light that indicates the camera is active from switching on.[87] In one widely reported incident, a hacker gained access to an Internet-connected baby monitor and used that access both to speak to the baby and to activate the included camera.[88]

In a variation on this theme, the owner of a laptop computer installs remote-control software on it and uses the camera to spy on a person who is using the computer. This has given rise to lawsuits in several situations. Aaron's, a chain of rent-to-own stores, installed software called PC Rental Agent on laptop computers that it rented to individuals. The purpose of the software, which allowed the person who controlled it

---

[83] EXEC. OFFICE OF THE PRESIDENT, *supra* note 59, at 2.

[84] Complaint, *In re* TRENDnet Inc., No. C-4426 (F.T.C. Jan. 16, 2014).

[85] The complaint charged TRENDnet with deception, by falsely representing that its cameras were secure, and unfairness, by failing to provide reasonable security, both in violation of Section 5 of the FTC Act. *Id.* The case settled, with TRENDnet agreeing to implement a comprehensive security program. Decision and Order, *In re* TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014).

[86] LORI ANDREWS ET AL., DIGITAL PEEPHOLES 8 (2015) (discussing use of fake media, spear phishing, ad spamming, and fake video games to install the software).

[87] *Id.* at 7.

[88] Babak D. Beheshti, *Smart Devices Undone by Dumb Security*, WALL ST. J., June 2, 2016, at A13. For other similar incidents, see Nate Anderson, *Webcam Spying Goes Mainstream as Miss Teen USA Describes Hack*, ARSTECHNICA (Aug. 16, 2013), https://arstechnica.com/tech-policy/2013/08/webcam-spying-goes-mainstream-as-miss-teen-usa-describes-hack/ (explaining that a hacker took pictures of Miss Teen USA through her webcam and tried to extort her to perform specified acts); Craig Silverman, *7 Creepy Baby Monitor Stories That Will Terrify All Parents*, BUZZFEED (July 24, 2015), https://www.buzzfeed.com/craigsilverman/creeps-hack-baby-monitors-and-say-terrifying-thing (describing several incidents).

both to disable the computer and to turn on the camera remotely, was to help in recovering the computer if the renter did not make the required payments or if it was stolen.[89] When Brian and Crystal Byrd learned that the Aaron's franchise that sold one of these computers to them had activated the camera hundreds of times in a one-month period with no disclosure to them (including while Crystal was using it dressed only in her underwear), they asserted federal and state law claims in a class-action lawsuit against Aaron's, many of its franchisees, and the maker of the PC Rental Agent software.[90] Aaron's agreed to pay $28.4 million to settle claims asserted by the State of California[91] and also settled an FTC action.[92]

In another incident, employees of a school district in Pennsylvania secretly took photographs of high school students by remotely activating the webcams in their school-issued laptop computers.[93] The cameras captured images of the students while they were at home, including in their bedrooms. The students filed a class action lawsuit against the school district, alleging violations of the Wiretap Act, the Computer Fraud and Abuse Act, the Stored Communications Act, the Fourth Amendment, and related state laws.[94] The school district settled, agreeing to pay $610,000.[95]

In 2010, a college student used the webcam on his laptop computer to spy on his roommate, discovering him kissing another man. The student publicized the information on Twitter, and his roommate responded by committing suicide.[96] The student who activated the camera, Dharun Ravi, was convicted on multiple counts, including invasion of privacy and bias intimidation, and was sentenced to thirty days in jail.[97]

---

[89] *Lawsuit: PC Rental Agent Spies on Users*, CBS NEWS (May 3, 2011), https://www.cbsnews.com/news/lawsuit-pc-rental-agent-spies-on-users/.

[90] Complaint, Byrd v. Aaron's, Inc., No. 1:11-cv-00101 (W.D. Pa. May 3, 2011); Corrected Third Amended Class Action Complaint at 1, Byrd v. Aaron's, Inc., No. 1:11-cv-00101 (W.D. Pa. Oct. 2, 2013). The litigation is ongoing.

[91] Press Release, Cal. Dep't of Justice, Attorney Gen. Kamala D. Harris Reaches $28.4 Million Settlement with Rental Business over Spyware, Unfair Business Practices (Oct. 13, 2014), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-reaches-284-million-settlement-rental-business.

[92] Complaint, *In re* Aaron's, Inc., No. C–4442 (F.T.C. Mar. 10, 2014). This case is discussed *infra*, text accompanying notes 505–13.

[93] Daniel Nasaw, *US School District Spied on Students Through Webcams, Court Told*, GUARDIAN (Feb. 19, 2010), https://www.theguardian.com/world/2010/feb/19/schools-spied-on-students-webcams.

[94] Complaint, Robbins v. Lower Merion Sch. Dist., No. 2:10-cv-00665-JD (E.D. Pa. Feb. 16, 2010).

[95] *Lower Merion School District Settles Webcam Spying Lawsuits for $610,000*, HUFFINGTON POST (Dec. 11, 2010), http://www.huffingtonpost.com/2010/10/11/lower-merion-school-distr_n_758882.html. The settlement also applied to another lawsuit based on the same conduct. *Id.*

[96] Ian Parker, *The Story of a Suicide*, NEW YORKER (Feb. 6, 2012), http://www.newyorker.com/magazine/2012/02/06/the-story-of-a-suicide.

[97] The convictions on the counts charging Ravi with bias intimidation were overturned on due process grounds. State v. Ravi, 147 A.3d 455, 458–59 (N.J. Super. Ct. App. Div. 2016).

Privacy issues also arise from IoT devices with audio capture capabilities. In 2015, Mattel released Hello Barbie, a Barbie doll that incorporates both a microphone and a speaker.[98] When a child (or anyone else) speaks to the doll, her voice is picked up by the microphone and sent via the Internet to ToyTalk, a company in San Francisco that uses speech recognition technology to convert the speech to text and artificial intelligence to devise an appropriate response. The captured speech is retained for possible additional use; the doll's privacy policy states that it may be used by third parties for "research and development purposes." A feature that child psychologists may find alarming allows parents to access the child's recorded conversations with the doll.[99] A class action lawsuit filed against Mattel and ToyTalk alleged violations of the Children's Online Privacy Protection Act ("COPPA"), common law intrusion upon seclusion, and a state law requiring consent before recording confidential communications.[100] German authorities have banned a doll called My Friend Cayla, which has similar capabilities, on privacy grounds.[101]

People may invite IoT devices into their home without realizing that they are connected to the Internet. For example, digital video recorders are likely to be connected to the Internet and to collect information about our television viewing activities: which shows we watch and record, how long we watch them, and more.[102]

---

Ravi subsequently accepted a plea deal and was sentenced to time served. Nate Schweber & Lisa W. Foderaro, *Roommate in Tyler Clementi Case Pleads Guilty to Attempted Invasion of Privacy*, N.Y. TIMES (Oct. 27, 2016), https://www.nytimes.com/2016/10/28/nyregion/dharun-ravi-tyler-clementi-case-guilty-plea.html.

98 Lauren Walker, *Hello Barbie, Your Child's Chattiest and Riskiest Christmas Present*, NEWSWEEK (Dec. 15, 2015), http://www.newsweek.com/2015/12/25/hello-barbie-your-childs-chattiest-and-riskiest-christmas-present-404897.html.

99 *Id.*

100 First Amended Class Action Complaint, Archer-Hayes v. ToyTalk, Inc., No. BC603467 (Cal. Super. Ct. Feb. 26, 2016). The case was later removed to federal court and dismissed after a settlement on undisclosed terms.

101 Kimiko de Freytas-Tamura, *The Bright-Eyed Talking Doll That Just Might Be a Spy*, N.Y. TIMES (Feb. 17, 2017), https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html. The Electronic Privacy Information Center filed a complaint against the manufacturer of the doll with the FTC, alleging that the doll's operation violates COPPA. Complaint and Request for Investigation, Injunction, and Other Relief, *In re* Genesis Toys (filed with F.T.C. Dec. 6, 2016). Alarmed by reports of data breaches related to connected toys, a congressional committee gathered information from manufacturers of the toys and issued a report recommending stronger efforts to prevent unauthorized disclosure of PII collected from children using these toys. OFFICE OF OVERSIGHT & INVESTIGATIONS, MINORITY STAFF REPORT, S. COMM. ON COM., SCI., & TRANSP., CHILDREN'S CONNECTED TOYS: DATA SECURITY AND PRIVACY CONCERNS (2016), https://www.billnelson.senate.gov/sites/default/files/12.14.16_Ranking_Member_Nelson_Report_on_Connected_Toys.pdf.

102 TiVo's privacy policy discloses that it collects various types of information from users of its DVR:

> We collect information (both automatically and when we ask you to provide it) when you use TiVo products . . . . Information we automatically collect may include, for example, data about your viewing behavior (such as how you use, watch, record, rate and interact with content accessed on or through TiVo products), device (such as model

VCRs, the predecessor of DVRs, were typically only connected to the television set and collected no information about us.

The current generation of smart television sets is another example of a stealth IoT device. These devices may collect an astounding range of information about their users by tracking their viewing habits and by capturing data using their built-in microphones and cameras.[103] According to the privacy policy accompanying a Samsung television:

> It logs where, when, how and for how long you use the TV. It sets tracking cookies and beacons designed to detect "when you have viewed particular content or a particular email message." It records "the apps you use, the websites you visit, and how you interact with content." It ignores "do-not-track" requests as a considered matter of policy.
>
> It also has a built-in camera—with facial recognition. The purpose is to provide "gesture control" for the TV and enable you to log in to a personalized account using your face. . . . The TV boasts a "voice recognition" feature that allows viewers to control the screen with voice commands. But the service comes with a rather ominous warning: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party."[104]

Most people probably do not expect that their television sets, like the "telescreens" in George Orwell's novel *1984*, will be spying on them.[105] The voice capture and transmission feature of the Samsung television set prompted the California legislature to enact a statute that regulates the use of these technologies.[106] VIZIO, the world's

---

number, software versions, and unique device identifiers), location (such as GPS data, zip code, and time zone), and cable service (such as cable provider and cable channels).

*Privacy Policy*, TIVO, https://www.tivo.com/legal/privacy (last visited Mar. 7, 2018). The policy also explains how that data may be used: "[W]e may use information we collect to: analyze your viewing habits (which lets us do things like suggest a particular TV show or movie that you may enjoy); [and] show you more relevant ads (both on TiVo products and on third-party websites)." *Id.* Digital media streaming devices may do likewise. *See* Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312 (N.D. Ga. 2015) (describing content provider's transmission of the user's unique identification to third parties to facilitate targeted advertising).

[103] Michael Price, *I'm Terrified of My New TV: Why I'm Scared to Turn This Thing On—and You'd Be, Too*, SALON (Oct. 30, 2014), https://www.salon.com/2014/10/30/im_terrified_of_my_new_tv_why_im_scared_to_turn_this_thing_on_and_youd_be_too/.

[104] *Id.*

[105] Former Ontario privacy commissioner Ann Cavoukian put it this way: "People expect to guide channels on TV with their voice. What they don't expect is a stupid device that can potentially capture all their conversations. Really, who would even think that?" Matt Kwong, *Samsung SmartTV an "Absurd" Privacy Intruder, Ann Cavoukian Says*, CBC NEWS (Feb. 10, 2015), http://www.cbc.ca/news/technology/samsung-smarttv-an-absurd-privacy-intruder-ann-cavoukian-says-1.2950982.

[106] CAL. BUS. & PROF. CODE § 22948.20–.25 (West 2016). The statute requires prominent notice to the user (but does not require her consent) before operating the voice recognition feature of a connected television set. *Id.* § 22948.20(a). It also prohibits using "[a]ny actual recordings of spoken word collected through the operation of a voice recognition feature" for

second-largest manufacturer of connected televisions, has also gotten into hot water over the feature of its televisions that tracks what is being watched and sends that information to third parties both to use for targeted marketing and to link the consumer's television viewing with his accessing of websites.[107] The FTC charged VIZIO with deception and unfairness,[108] and a class action against VIZIO is pending.[109]

Another category of IoT devices that raises serious privacy issues is wearables. These include fitness trackers,[110] connected watches,[111] action cameras,[112] blood pressure monitors,[113] fertility trackers,[114] running data trackers,[115] caloric intake trackers,[116] and sports concussion monitors.[117] The ultimate wearables are implantable medical devices: pacemakers[118] and insulin pumps.[119]

Some of these devices collect data that can reflect the user's health condition. This information may have substantial commercial value to entities such as health insurance companies and the individual's employer. Like smartphones and mobile computing devices, wearable devices often are capable of sensing their location through GPS and other geolocation technologies.[120] As noted above,[121] one's location at a given time can be highly revealing. These devices tend to be used by a single

---

advertising purposes (but does not prohibit such use of the data that may be extracted from the recordings). *Id.* § 22948.20(b)–(c); *see also* Michael Silvestro & John Black, *"Who Am I Talking To?"—The Regulation of Voice Data Collected by Connected Consumer Products*, BUS. L. TODAY (May 2016), http://www.americanbar.org/publications/blt/2016/05/06_black.html.

107 FTC v. VIZIO, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017).

108 *Id.* The case is discussed *infra*, text accompanying notes 499–504.

109 *In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204 (C.D. Cal. 2017).

110 FITBIT, https://www.fitbit.com/ (last visited Mar. 7, 2018).

111 APPLE WATCH, https://www.apple.com/watch/ (last visited Mar. 7, 2018).

112 GOPRO, https://gopro.com/ (last visited Mar. 7, 2018).

113 *Premium Wireless Blood Pressure Monitor*, A&D MEDICAL, http://www.andonline.com/medical/products/details.php?catname=Blood_Pressure&product_num=UA-651BLE (last visited Mar. 7, 2018).

114 TEMPDROP, http://www.temp-drop.com/ (last visited Mar. 7, 2018).

115 RUNSCRIBE, http://www.runscribe.com/ (last visited Mar. 7, 2018).

116 HEALBE, http://healbe.com/ (last visited Mar. 7, 2018).

117 LINX IAS, http://linxias.com/ (last visited Mar. 7, 2018).

118 *Our Pacing Systems: Bradyarrhythmia Management*, MEDTROINC, http://www.medtronic.com/us-en/healthcare-professionals/products/cardiac-rhythm/pacemakers.html (last visited Mar. 7. 2018).

119 TANDEM, https://www.tandemdiabetes.com/ (last visited Mar. 7, 2018).

120 Lisa Eadicicco, *A New Wave of Gadgets Can Collect Your Personal Information Like Never Before*, BUS. INSIDER (Oct. 9, 2014), http://www.businessinsider.com/privacy-fitness-trackers-smartwatches-2014-10.

121 *See supra* note 52 and accompanying text.

individual rather than a household, so the data they collect may be more easily identified to an individual.

An example of an IoT device that collects data that may not be recognized as potentially privacy-invading is smart electricity meters in the home. Smart meters are a key component of the Smart Grid, the term for a modernized national electricity transmission system that uses information and other technologies to improve the system's performance.[122] Two features of a smart meter distinguish it from a traditional electrical meter. First, a smart meter records an electricity consumer's usage data over more-or-less brief intervals, which may range from an hour down to as little as a second or two; by contrast, ordinary meters record usage data no more frequently than the duration of a billing period, typically a month for residential users.[123] Second, a smart meter transmits the data it collects to the utility automatically, usually via wireless transmission; traditional meters rely on a meter-reader to visit the premises and to read and record the meter's display.[124] In addition to helping enable better management of the grid, smart meters and the smart grid can help consumers by enabling them to shift consumption to lower-priced off-peak times and to switch off appliances remotely via the Internet.[125]

The rollout of smart residential meters is proceeding apace. The number of smart meters installed in the United States has risen from 6.7 million in 2007 to 58.5 million in 2014; as a percentage of all meters, the corresponding figures are 4.7% and 40.6%.[126] The decision to replace a traditional meter with a smart meter is made by the utility, and the residential customer generally is given no choice.[127]

---

[122] *See* Samuel J. Harvey, *Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid*, 61 UCLA L. REV. 2068, 2072 (2014) ("Generally, the smart grid involves computerizing and automating the existing system by introducing two-way digital communication between grid operators and sites throughout the grid."). The Energy Independence and Security Act of 2007, Pub. L. No. 110-140, 121 Stat. 1492 (codified at 42 U.S.C. §§ 17001–17386), established a federal policy of fostering development of the Smart Grid. The statute includes a list of ten features that characterize the Smart Grid, including "[i]ncreased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid" and "[d]eployment of 'smart' technologies . . . for metering, communications concerning grid operations and status, and distribution automation." 42 U.S.C. § 17381(1), (5).

[123] Naperville Smart Meter Awareness v. City of Naperville, No. 11 C 9299, 2013 WL 1196580, at *1 (N.D. Ill. Mar. 22, 2013).

[124] *Id.* ("A smart meter is a device that has the ability to collect aggregate, as well as detailed, measurements of a customer's electrical power usage and to communicate those measurements via wireless radio frequency ('RF') to the electric utility provider.").

[125] Harvey, *supra* note 122, at 2073.

[126] *See* FED. ENERGY REG. COMM'N, STAFF REPORT, ASSESSMENT OF DEMAND RESPONSE AND ADVANCED METERING 3 (2016), https://www.ferc.gov/legal/staff-reports/2016/DR-AM-Report2016.pdf. These figures reflect combined residential, industrial, and commercial installations. *Id.* at 4.

[127] Some utilities will allow a customer to keep the traditional meter, but will charge an additional monthly fee to reflect the additional costs of sending out a meter-reader. *See Report of the Demand-Side Resources & Smart Grid Committee*, 34 ENERGY L.J. 373, 381–85 (2013). New Hampshire is unusual in that a smart meter may not be installed at a residence or business unless the customer opts in by submitting a written consent form. *Id.* at 383.

The granularity of data collected by smart meters gives rise to potential privacy issues. Electrical appliances exhibit particular usage profiles, and these can be identified from the data that smart meters send to the utility. For example, a refrigerator cycles on and off, generating a recognizable pattern. An oven also cycles during use, but at a higher level of usage and with a different pattern. Other usage patterns can be associated with washing machines, tea kettles, and television sets.[128] Data collected from a residential smart electricity meter can reveal when the occupants eat, shower, and watch television; the residents' work schedule, sleeping patterns, and other lifestyle habits; how many people are living at the house; whether anybody is home; and where they are located in the house.[129] An employee of Siemens Energy has noted that data collected from smart meters can be used to "infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data."[130]

Newer technologies will reveal even more information about appliance usage occurring within a residence. When appliances are connected into a Home Area Network ("HAN"), they will communicate very detailed information about their functioning:

> [A] HAN-enabled appliance transmits specific information related to the use of that individual appliance. A HAN-enabled clothes washing machine can transmit the time of day a consumer washes his or her clothes as well as the wash cycle and water temperature settings. While utility companies or third party energy manage service providers can collect this information under the guise of energy efficiency management, this information can also reveal very private, personal consumer habits.[131]

Inferences drawn from data that smart meters collect may be of interest to a wide range of parties. Consider the following:

- Insurance companies might be interested in a policyholder's behavior patterns, like trouble sleeping or lack of physical activity, which could indicate possible health problems, in order to price premiums or decide whether to insure.[132]

---

[128] NAT'L INSTIT. OF STANDARDS & TECH., 2 GUIDELINES FOR SMART GRID CYBER SECURITY 13 (2010).

[129] *Id.*

[130] Gerard Wynn, *Privacy Concerns Challenge Smart Grid Rollout*, REUTERS (June 25, 2010), http://www.reuters.com/article/2010/06/25/energy-smart-idUSLDE65N2CI20100625.

[131] *Resolution on Privacy and Security Related to Smart Meters*, TRANS ATLANTIC CONSUMER DIALOGUE (June 2011), https://epic.org/privacy/smartgrid/Smart_Meter_TACD_Resolution_FINAL.pdf.

[132] NAT'L INSTIT. OF STANDARDS & TECH., *supra* note 128, at 30. Lee Tien, *New "Smart Meters" for Energy Use Put Privacy at Risk*, EFF (Mar. 10, 2010), https://www.eff.org/deeplinks/2010/03/new-smart-meters-energy-use-put-privacy-risk.

- Law enforcement authorities can analyze electricity usage patterns to determine whether residents are present and make inferences about activities occurring inside the home.[133]
- It may be helpful in civil litigation for a party to be able to demonstrate that residents were at home at a particular time or the number of people present.[134]
- The press can always use more data to gratify the public's interest in the activities of celebrities.[135]
- Creditors might be interested in knowing details about a borrower's behavior that may have a bearing on creditworthiness.[136]
- Burglars could use information from electricity usage or the feed from in-home security cameras to determine whether residents are present.[137]

### *B. Use of the Data*

The most common use of the data that is collected in these ways is to fuel interest-based advertising.[138] The data is subjected to analysis, yielding inferences about an individual's likes and interests.[139] Automated systems then select an advertisement to show to that individual based on the premise that she is more likely to respond favorably to an advertisement selected in this way than to one selected without regard to her interests.[140] Advertising via older media, such as television and print, can be roughly targeted by selecting an advertising vehicle based on the demographics of the

---

[133] NAT'L INSTIT. OF STANDARDS & TECH., *supra* note 128, at 30.

[134] *Id.*

[135] *Id.*

[136] *Id.* at 31.

[137] *Id.*

[138] "Interest-based advertising" is a more recent term for what has previously been called "online behavioral advertising" and "online profiling." *See* FED. TRADE COMM'N STAFF, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 46 (2009) [hereinafter FTC STAFF, SELF-REGULATORY PRINCIPLES], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf (defining "online behavioral advertising" as "the tracking of a consumer's online activities *over time*—including the searches the consumer has conducted, the web pages visited, and the content viewed—in order to deliver advertising targeted to the individual consumer's interests"); FTC, ONLINE PROFILING, *supra* note 40, at 2–6 (explaining how online profiling works). "Interest-based advertising" is sometimes used more broadly than the other terms to reference targeting based on both online and offline activity.

[139] *Understanding Online Advertising*, NETWORK ADVERT. INITIATIVE, https://www.networkadvertising.org/understanding-online-advertising/how-does-it-work (last visited Mar. 8, 2018).

[140] *See* FTC STAFF, SELF-REGULATORY PRINCIPLES, *supra* note 138, at 2–3.

medium's audience.[141] Interest-based advertising allows the targeting to be much more granular, down to the level of a particular individual.

The most sophisticated targeted advertising is based on the application of analytics to PII that has been centralized in the hands of data brokers. Data brokers obtain their information from multiple sources.[142] Typically, very little of that information comes directly from the data subjects. Most comes from government sources (both federal and state),[143] other public sources (such as telephone books and news reports), and commercial sources (such as retailers and magazine publishers).[144] Information also comes from individuals' own public postings on social media sites, blogs, and other online venues.[145] The amount of information that data brokers hold is massive: hundreds of billions of data points covering nearly all consumers in the United States, with up to 3,000 data points for each individual.[146] As early as 1996, data brokers held data "on almost all households in the United States."[147]

Data brokers analyze all this information and draw inferences about an individual's preferences. They then sell this "derived data" to their clients—typically companies that wish to identify potential customers for their products.[148] The companies may then target their marketing efforts based on this information.[149]

## III. PROTECTING PRIVACY THROUGH LEGAL RULES AND VOLUNTARY PRACTICES

In the United States, the rules protecting information privacy are frequently described as "sectoral."[150] What this term signifies is that, unlike in other legal systems,[151] the United States does not have any scheme of legally enforceable rules

---

[141] *3 Stats About Traditional Media Audiences to Keep in Mind This Coming Year*, MARKETING CHARTS (Dec. 29, 2016), https://www.marketingcharts.com/industries/media-and-entertainment-73322.

[142] FTC, DATA BROKERS, *supra* note 29, at 11.

[143] The federal government supplies data brokers with information such as the demographics of residents at the city-block level, postal change-of-address information, and bankruptcy filings. State governments can provide information from records pertaining to real estate, voter registration, motor vehicles, courts, birth, marriage, divorce, and death. *Id.* at 11–12.

[144] *Id.* at 13.

[145] *Id.*

[146] *Id.* at 46–47.

[147] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 20 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON] (citing ARTHUR M. HUGHES, THE COMPLETE DATABASE MARKETER 354 (2d ed. 1996)).

[148] FTC, DATA BROKERS, *supra* note 29, at 19.

[149] *Id.* at 25 ("The client identifies the attributes that it would like to find in a consumer audience, and the data broker provides a list of consumers with those attributes.").

[150] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 908–16 (2009) (tracing the development of the United States' sectoral approach and contrasting it with the European Union's omnibus approach).

[151] The most prominent example is the European Union. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive], discussed *infra* text accompanying notes

that protect privacy generally. Instead, the United States has laws that apply to particular contexts, or "sectors," that legislators have thought warranted special treatment. The sectors that have qualified for this treatment under federal law include finance,[152] health,[153] education,[154] video rentals,[155] driver's licenses,[156] and aspects of online privacy.[157] Privacy law at the state level protects against intrusion into one's private sphere, public disclosure of private facts, publication of facts that place one in a false light, and unauthorized use of a person's likeness for commercial purposes, as well as some of the sectors addressed by federal law.[158]

Alongside these legally enforceable rules sit various sets of principles that have been constructed to encapsulate a normative view of how information privacy *should* be protected. Generally referred to as the Fair Information Principles or Fair Information Practice Principles ("FIPPs"), these statements have served as a source of inspiration for legislation and as recommended best practices for voluntary implementation.[159]

The core ideology underlying the FIPPs, as well as nearly all of the laws governing information privacy, is that privacy protection is a matter for the informed choice of the data subject.[160] This is structured laissez-faire, which places no substantive

248–56; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR], discussed *infra* text accompanying notes 257–63.

[152] *E.g.*, Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2018), discussed *infra* text accompanying notes 268–77; Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3408 (2018).

[153] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 56 (codified as amended in scattered sections of 29 U.S.C.) (2018).

[154] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232 (2018).

[155] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2018).

[156] Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2018).

[157] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2018); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2018); Stored Communications Act, 18 U.S.C. § 2703 (2018).

[158] These are usually classed together as the privacy torts, which developed through common law and have been codified in the law of many states. *Privacy and Business: The Privacy Torts*, PRIVACILLA (Dec. 19, 2000), http://www.privacilla.org/business/privacytorts.html.

[159] Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIVACY FORUM (Jan. 4, 2008), https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

[160] FED. TRADE COMM'N, PRIVACY ONLINE 7 (1998) [hereinafter FTC, PRIVACY ONLINE], https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf ("The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed below—

shackles on the hands of entities that seek to collect and use PII. Decisions affecting information privacy are to be made under the usual rules of the marketplace, where two parties engage in a negotiation and arrive at a bargain. The only imposed structure is the insistence that the prospective data collector must supply the prospective data subject with information that is deemed relevant to the latter's decision.

This is a deviation from the usual market slogan of *caveat emptor*: a seller is generally under no obligation to supply the buyer with information about products it offers.[161] It is the buyer's burden to seek out information he deems relevant to his purchase decision, or else assume the risk that he will regret the purchase. The FIPPs, by contrast, include a notice requirement: the information collector must disclose to the data subject relevant facts about its collection and use of PII. A rule requiring a company to disclose its privacy practices fits comfortably within a recognized exception to the no-required-disclosure rule, namely the "special facts" doctrine, which "places a duty to disclose on one with specialized knowledge not available to the other party."[162] What PII the collector will use, and the uses to which the PII will be put, are facts that are quintessentially in the hands of one party and (in the absence of disclosure) not available to the other.[163]

The notice-and-choice paradigm is thus situated squarely within the intellectual construct of market exchange. The seller offers a product or service for sale in the marketplace. Because the seller has special access to information about the transaction that may be material to the prospective purchaser—what PII the seller will collect in the course of the transaction and how it will use that PII—the seller must disclose this information to the purchaser. Based on that information, and whatever other information about the product that the purchaser has acquired by his own efforts in line with the doctrine of *caveat emptor*, the purchaser makes an informed decision whether to engage in the transaction and thereby allow collection of his PII.

---

choice/consent, access/participation, and enforcement/redress—are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.").

[161] *See* Nicola W. Palmieri, *Good Faith Disclosures Required During Precontractual Negotiations*, 24 SETON HALL L. REV. 70, 109–12 (1993) (describing the origins of *caveat emptor* in legal doctrine).

[162] *Id.* at 132.

[163] Disclosure requirements have been enacted in a variety of contexts exhibiting information asymmetries. For example, many states have enacted mandatory disclosure laws that require sellers of real estate to disclose known defects to the buyer. *See* Alan M. Weinberger, *Let the Buyer Be Well Informed?—Doubting the Demise of Caveat Emptor*, 55 MD. L. REV. 387, 415–16 (1996). Advertisers must disclose information that is needed to prevent a claim from being misleading. *See* FED. TRADE COMM'N, .COM DISCLOSURES: HOW TO MAKE EFFECTIVE DISCLOSURES IN DIGITAL ADVERTISING 5 (2013) [hereinafter FTC, .COM DISCLOSURES], https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf. The Securities Act requires issuers of securities to make prescribed disclosures in a registration statement that is filed with the Securities and Exchange Commission and made publicly available. *Registration Under the Securities Act of 1933*, U.S. SEC. & EXCH. COMM'N (Sept. 2, 2011), https://www.sec.gov/fast-answers/answersregis33htm.html. Most prepared foods must be labeled with ingredients and nutrition information. *Food Labeling Guide*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/Food/GuidanceRegulation/GuidanceDocumentsRegulatory Information/ LabelingNutrition/ucm2006828.htm.

In what follows in Section III(A), I first set out the notice-and-choice principles as they have appeared in different formulations starting with their initial statement in 1973. In Section III(B), I then show how those principles have been applied in positive law and, in Section III(C), in self-regulatory schemes.

### *A. Statements of Fair Information Practice Principles*

The notice-and-choice paradigm originated forty-five years ago as a recommendation to Congress in a report that was the product of a committee constituted to examine the new issues raised by automated data processing. Notice and choice are also present in numerous other formulations of the FIPPs that have appeared in the succeeding decades.

#### 1. The 1973 HEW Report

The first influential statement of the principles that should govern the collection and use of PII is contained in a 1973 report entitled *Records, Computers, and the Rights of Citizens*.[164] In the early 1970s, there was widespread public concern "that automated personal data systems present a serious potential for harmful consequences, including infringement of basic liberties," specifically "privacy and due process."[165] This concern motivated the Secretary of the Department of Health, Education, and Welfare, Elliot L. Richardson, to establish a committee tasked with making recommendations about how to ameliorate these risks.[166] This report is frequently cited as the original source of the concept of fair information practices, including notice-and-choice.[167]

The report sets out what it calls the five "fundamental principles of fair information practice"[168] and recommends that rules based on these principles be enacted into law

---

[164] HEW REPORT, *supra* note 22. On the influence of the report, see Suzanne M. Thompson, *The Digital Explosion Comes with a Cost: The Loss of Privacy*, 4 J. TECH. L. & POL'Y 3, 33 (1999) (stating that the proposed Code of Fair Information Practices "has been very influential in setting the tone and content of laws that limit access to and use of personal information" and was embodied in the Privacy Act of 1974).

[165] HEW REPORT, *supra* note 22, at viii (quoting a determination by Elliot L. Richardson, Secretary of Health, Education, and Welfare).

[166] *Id*. (describing establishment of the Secretary's Advisory Committee on Automated Personal Data Systems); *see* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1164–65 (2002) (citing expressions of concern about the privacy implications of computerized databases from the 1960s and 1970s).

[167] *See, e.g.*, WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 9 n.9 (2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf (stating that the report's proposed Code of Fair Information Practices "established the framework on which much privacy policy would be built"); SIMSON GARFINKEL, DATABASE NATION 7 (1st ed. 2000) (describing the Code as "the most significant American thinking on the topic of computers and privacy to this day"); FTC, PRIVACY ONLINE, *supra* note 160, at 48 n.27 (stating that the Fair Information Practice Principles "were first articulated in a comprehensive manner" in the HEW Report).

[168] HEW REPORT, *supra* note 22, at 41. This report is evidently the source of the term "fair information practices," modeled on the term "fair labor practices." *See* Willis H. Ware, RAND and the Information Evolution 157 (2008), *quoted in* Robert Gellman, Fair Information Practices: A Basic History (ver. 2.16 June 17, 2016). The term "unfair labor practices" was a

as a Code of Fair Information Practice ("Code")[169]—a recommendation that was not followed.

The principles include a rather limited statement of notice-and-choice. The relevant principle states what would later be referred to as "purpose specification."[170] It reads: "There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."[171] The provisions of the proposed (but not enacted) Code implement a somewhat broader notice-and-choice rule. First, the Code says that a collector of PII must (1) inform the data subject whether he has any choice about whether to supply the requested information, and (2) if choice is available, inform the data subject what will be the consequences to him of declining to provide the requested information.[172] Second, the Code says that if the collector wishes to use the PII in a manner that is inconsistent with the purpose for its collection, it must first obtain the data subject's informed consent.[173] The requirement of "informed" consent implies that the data subject must receive notice of the intended use. The proposed code does not, however, specify what would constitute consent: is a failure to object (opt-out) sufficient, or does consent require some affirmative manifestation of consent (opt-in)?

2. The 1977 Report of the Privacy Protection Study Commission

The Privacy Act of 1974 established the Privacy Protection Study Commission, which Congress charged with studying the privacy issues that arise in the context of automated data processing and making legislative recommendations.[174] The commission's report finds that individuals should receive better notice of an organization's information-collection practices so that they may exercise informed choice about whether to consent to that collection.[175]

Among the numerous recommendations in the 600-page report is one calling for voluntary implementation of a notice-and-choice procedure by entities that rent data from their mailing lists to other companies for use in direct-mail solicitations.[176]

---

familiar one at the time the report was written, used extensively in the National Labor Relations Act (1935).

169 HEW REPORT, *supra* note 22, at 50.

170 *See, e.g.*, OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA ¶ 9 (1980) [hereinafter OECD, GUIDELINES].

171 HEW REPORT, *supra* note 22, at 41.

172 *Id.* at 59. The text refers to "legally required" submissions of data and thus seems to envision that the data collector will be a government agency, but the report's recommendations apply equally to the private sector. *Id.* at 50 (urging both government agencies and "private organizations" to voluntarily comply with the report's recommendations).

173 *Id.* at 61.

174 Privacy Act of 1974, 5 U.S.C. § 552a (2018). The Commission was set up as a means of addressing issues that were not resolved in the Privacy Act. *See* Alex Kardon, *Damages Under the Privacy Act: Sovereign Immunity and a Call for Legislative Reform*, 34 HARV. J.L. & PUB. POL'Y 705, 751–52 (2011).

175 PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 16 (1977).

176 *Id.* at 34.

Persons whose names appear on the list, as the list owner's "customers, members, or donors," are to be "informed" of the entity's list-rental practices, and each such person is to be "given an opportunity to indicate to the organization that he does not wish to have his address, or name and address, made available for such purposes."[177] This recommendation seems to envision opt-out choice: the individual need act only if he does *not* want his information disclosed.

### 3. The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

In 1980, the Organisation for Economic Co-operation and Development ("OECD") released its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which it characterizes as "the first internationally agreed-upon set of privacy principles."[178] The *Guidelines* prescribe notice-and-choice at two points in a transaction. First, at the time the information is initially collected, the data subject should receive notice of "[t]he purposes for which personal data are collected."[179] Although not clearly expressed, the general rule is that the collection should be done only with the consent of the data subject.[180] Second, subsequent uses of the data for purposes other than those for which it was collected are allowable without further notice to the data subject as long as those uses "are not incompatible with" the original purpose.[181] However, data are to be disclosed or used for incompatible purposes only "with the consent of the data subject" (or as provided by law).[182]

### 4. The 1995 Clinton Administration Internet Privacy Reports

In 1995, at the dawn of the commercial Internet,[183] two federal government agencies released reports that set out the position of President Bill Clinton's administration on how to address the new privacy issues that the new technology raised. In a white paper titled *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*,[184] the National Telecommunications and Information

---

[177] *Id.* at 151.

[178] OECD, THE OECD PRIVACY FRAMEWORK 19 (2013) [hereinafter OECD, PRIVACY FRAMEWORK].

[179] OECD, GUIDELINES, *supra* note 170, ¶ 9.

[180] The relevant principle states that data collection should be, "where appropriate, with the knowledge or consent of the data subject." *Id.* ¶ 7. The Explanatory Memorandum accompanying the Guidelines suggests that obtaining the data subject's consent will almost always be "appropriate," offering as examples of exceptions "[c]riminal investigation activities and the routine up-dating of mailing lists." OECD, PRIVACY FRAMEWORK, *supra* note 178, at 56.

[181] OECD, GUIDELINES, *supra* note 170, ¶ 9.

[182] *Id.* ¶ 10.

[183] The beginning of Internet commerce can be dated to the dropping of the NSF's Acceptable Use Policy. *See supra* note 34 and accompanying text.

[184] NAT'L TELECOMM. & INFO. ADMIN., PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995) [hereinafter NTIA, PRIVACY], https://www.ntia.doc.gov/legacy/ntiahome/privwhitepaper.html.

Administration ("NTIA"), a unit of the Department of Commerce, set out the administration's position on use of "telecommunications-related personal information" ("TRPI"), defined as "personal information that is created in the course of an individual's subscription to a telecommunications or information service or as a result of his or her use of that service."[185] This is metadata—information derived from a subscriber's use of telecommunications, such as a telephone call, an email message, or browsing the Web, that does not include the communicative content of the transaction. For a phone call, the TRPI would include the number called, the time of the call, and its duration, but not the content of the conversation.

The white paper states that its approach has "two fundamental elements—provider notice and customer consent."[186] No explicit notice or consent is required if the provider merely uses the TRPI for its intended purpose—to deliver the requested telecommunications service by connecting a call or transmitting an email or even to analyze the subscriber's usage to offer a service that the subscriber may prefer. The subscriber is assumed to be on notice of, and to have implicitly consented to, such expected uses.[187] But if the provider intends to use the TRPI for some other purpose, the white paper calls for the subscriber to be notified of that use[188] and given a choice whether to permit it.[189]

The data subject must receive notice at the initiation of the provider-subscriber relationship. The form in which the subscriber must convey his consent depends on the nature of the information that the provider proposes to use. If the information is "non-sensitive," then opt-out consent will suffice; but for unexpected uses of "sensitive" information, only opt-in consent will do.[190] The white paper does not propose a definition of "sensitive," but offers some examples: "information relating to health care (*e.g.*, medical diagnoses and treatments), political persuasion, sexual matters and orientation, and personal finances (*e.g.*, credit card numbers) should be considered 'sensitive.'"[191]

A working group of the Information Infrastructure Task Force, which Vice President Gore established to study a range of policy issues connected to cyberspace,[192] drafted the second of the two Clinton Administration policy papers on

---

[185] *Id.* at 5.

[186] *Id.* at 8.

[187] *Id.* at 22 ("When personal information is collected and used only to render a service, explicit notice may not be required because the individual is already aware of the extent of that information's collection and use.").

[188] *Id.* ("[T]elecommunications and information service providers should give their customers plain and conspicuous notice of any unrelated or ancillary use of their TRPI.").

[189] *Id.* at 23 ("[I]ndividuals should have the right to limit or prohibit ancillary or unrelated uses of personal information, such as disclosing information to third party marketers.").

[190] *Id.* at 25.

[191] *Id.* at 25 n.98.

[192] *See* INFO. POL'Y COMM., NAT'L INFO. INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE (Draft for Public Comment 1997), at text accompanying n.8, https://aspe.hhs.gov/report/options-promoting-privacy-national-information-infrastructure; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1205 n.40 (1998).

Internet privacy, titled *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*. The *Principles* call for an information collector to provide the data subject with notice consisting of "sufficient information to make an informed decision about his or her privacy," including the purpose for collecting the information, its expected use, and "[t]he consequences of providing or withholding information."[193] Once the data subject has exercised his choice and tendered the requested information, the collector is free to use it for purposes specified in the notice.[194] If the collector wants to use it in a manner that is incompatible with "the individual's objectively reasonable contemplation and scope of consent when the information was collected," then the collector must first obtain the data subject's consent.[195] As with the NTIA white paper, whether opt-out consent is sufficient or whether opt-in is required depends on the sensitivity of the information in question.[196]

5. The FTC's 1998, 1999, and 2000 Reports to Congress

In 1998, the FTC released a report on the current status of online privacy, with recommendations to Congress.[197] The report starts by asserting that privacy in online transactions should be governed by a set of "widely-accepted principles concerning fair information practices"—the FIPPs.[198] Those principles include what it calls "Notice/Awareness" and "Choice/Consent."[199] The notice principle calls for the information collector to disclose its "information practices" before collecting personal information, as "[w]ithout notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[200] The "information practices" requiring disclosure include the identity of the data collector, the anticipated uses and disclosures, the nature of the information collected, and the consequences of refusing to provide the information.[201]

The report states that choice does not apply to the initial collection of information, but rather that "choice relates to secondary uses of information—*i.e.*, uses beyond those necessary to complete the contemplated transaction."[202] The consumer is

---

[193] NAT'L INFO. INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE 6 (1995), https://aspe.hhs.gov/privacy-and-national-information-infrastructure-principles-providing-and-using-personal-information.

[194] *Id.*

[195] *Id.* at 7.

[196] *Id.* ("In some cases, the consequences to an individual may be so significant that the prospective data user should proceed only after the individual has specifically opted into the use by explicitly agreeing.").

[197] FTC, PRIVACY ONLINE, *supra* note 160.

[198] *Id.* at 7. The report cites the 1973 HEW Report as the original source of these principles. *Id.* at 48 n.27.

[199] *Id.* at 7–9.

[200] *Id.* at 7.

[201] *Id.* at 7–8.

[202] *Id.* at 8.

assumed to have exercised choice as to the initial collection by engaging in the transaction after receiving notice of the organization's information practices.

The report discusses the two main variations in choice procedure, opt-in and opt-out, but after offering a rather impractical suggestion of how the need for either might be avoided in online transactions does not express a preference for one over the other.[203]

The report castigates online businesses for failing to meaningfully implement the FIPPs; but the report also recommends that Congress take no action to require implementation of fair information practices via legislation, instead allowing the industry more time to self-regulate and promising to consider whether additional incentives to self-regulate might be called for.[204] In a follow-up report in 1999, the FTC noted that self-regulation had made some halting progress and recommended that industry be given more time to self-regulate.[205] But in 2000, the FTC, exasperated by the limited progress in implementation of the FIPPs that had come about via self-regulation, recommended that Congress step in and enact legislation that "would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites."[206] The recommendation called for implementation of notice-and-choice along the lines of the discussion contained in the 1998 report. However, the election of President George W. Bush in 2000 brought a change of leadership to the FTC, which disavowed the recommendation for legislation and suggested the need for further study.[207]

6. The Obama Administration's 2012 Consumer Privacy Bill of Rights

The Obama Administration offered its take on protecting online privacy in a 2012 White House report titled *Consumer Data Privacy in a Networked World*.[208] The report sets forth a Consumer Privacy Bill of Rights, which applies the FIPPs to commercial activity on the Internet. Notice and choice remain the foundational principles

[203] *Id.* at 9 ("The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.").

[204] *Id.* at 41–42. However, as to children's online privacy, the FTC did recommend legislation, and Congress responded by enacting the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2018). *Id.* at 42.

[205] FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE 12 (1999), https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf.

[206] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 36 (2000) [hereinafter FTC, FAIR INFORMATION PRACTICES], https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[207] Timothy J. Muris, Chairman, Fed. Trade Comm'n, Remarks at the Privacy 2001 Conference (Oct. 4, 2001), www.ftc.gov/speeches/muris/privisp1002.htm (stating that the agency no longer supported federal legislation to protect online privacy, having concluded there was a need "to develop better information about how such legislation would work and the costs and benefits it would generate").

[208] WHITE HOUSE, *supra* note 167. The report acknowledged that it was building on recommendations contained in a 2010 Department of Commerce green paper. *Id.* at 7.

governing the relationship between entities that collect and use private information and the data subjects to which that information pertains.[209] Some novelties are present in the terminology: notice is called "Transparency," choice is called "Individual Control" (or sometimes "Individual Choice"), and both principles undergo modification by application of the "Respect for Context" principle.[210] The idea that the rules for notice and choice should vary depending on context is one that appears in a limited way in some earlier formulations, such as by treating "sensitive" information differently from other personal information,[211] but the role of context is more pervasive in the Consumer Privacy Bill of Rights.

Still, it's all about notice-and-choice. Consumers should receive notice that enables them to make informed choices about their private information: "companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties."[212] Context determines how prominent the notice must be. For example, because ordering an item to be shipped requires providing a name and address to the shipper, the retailer need not give "prominent notice of the practice"—but the retailer still should describe the practice in its full privacy notice.[213] The choices that the company should offer are those "that are appropriate for the scale, scope, and sensitivity of personal data in question."[214] Thus, "companies that have access to significant portions of individuals' Internet usage histories, such as search engines, ad networks, and online social networks," should offer "fine-grained control of personal data use and disclosure"; but companies that collect data for statistical purposes only need not offer choice.[215] Even third-party users of PII that have no direct contact with the data subjects, such as data brokers, "should seek innovative ways to provide consumers with Individual Control."[216]

Whereas ordinary notice is required at the time the personal information is collected and choice must be offered if it cannot be inferred from the circumstances, a "heightened" form of notice-and-choice must be provided if subsequent uses of the data are inconsistent with the data subject's expectations.[217] The report does not say

---

[209] *Id.* at 1.

[210] *Id.* at 15.

[211] *See supra* text accompanying note 190 (noting that the NTIA white paper proposes differentiating between treatment of sensitive and non-sensitive information).

[212] WHITE HOUSE, *supra* note 167, at 14.

[213] *Id.* at 17. Likewise, the report considers that consumers will be aware that the retailer will use the data to market new products to the consumer as well as for "analyzing how consumers use a service in order to improve it, preventing fraud, complying with law enforcement orders and other legal obligations, and protecting intellectual property." Consent as to these uses may therefore be inferred. *Id.*

[214] *Id.* at 11.

[215] *Id.* at 11–12.

[216] *Id.* at 13.

[217] *Id.* at 15 (stating that if companies wish to use PII for purposes that are not "consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data," they should "provide heightened Transparency and Individual

what would constitute "heightened" notice and choice, other than to observe that the requirements "may be more stringent than was necessary at the time of collection."[218] A discussion draft of a bill that would enact the Consumer Privacy Bill of Rights fleshes out the concept only modestly, in the process revealing its hollowness: heightened notice means notice that is provided "at times and in a manner reasonably designed to enable individuals to decide whether to reduce their exposure to the associated privacy risk," while heightened choice requires "a mechanism for control that is reasonably designed to permit individuals to exercise choice to reduce such privacy risk."[219] This is no more than to say that "heightened" notice and choice is that which provides data subjects with effective notice and choice—what one could be forgiven for thinking is inherent in the concept of *non*-heightened notice and choice.

7. The FTC's 2012 Report, Protecting Consumer Privacy in an Era of Rapid Change

As discussed above, during the late 1990s, the FTC issued a series of reports that promoted notice-and-choice as the preferred framework for handling online privacy. That era came to an end when Congress failed to act on the FTC's 2000 recommendation for legislation implementing notice-and-choice, and the FTC's new chairman disavowed the recommendation.[220] The FTC's online privacy efforts then shifted to bringing enforcement actions under its existing statutory authorities[221] and to promoting various schemes of self-regulation.[222]

The FTC resumed its policy-oriented work on online privacy by convening a series of roundtable discussions starting December 2009, culminating in the issuance of a 2012 report titled *Protecting Consumer Privacy in an Era of Rapid Change*.[223] The report sets forth a "privacy framework" that is based on notice-and-choice.[224] But the report contains some striking divergences from the FTC's previous expositions of

Choice by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection").

[218] *Id.* at 16.

[219] Administration Discussion Draft: Consumer Privacy Bill of Rights Act § 103(b)(1) (Feb. 27, 2015). An analysis of the bill by the Center for Democracy and Technology says that "heightened" consent means opt-in, but the inference is a weak one because the bill does not mention either opt-in or opt-out. *Analysis of the Consumer Privacy Bill of Rights Act*, CTR. FOR DEMOCRACY & TECH. (Mar. 2, 2015), https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/. For criticism of the heightened notice and choice framework, see James P. Nehf, *Protecting Privacy with "Heightened" Notice and Choice*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 475 (John A. Rothchild ed., 2016).

[220] Muris, *supra* note 207.

[221] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 8–9 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf (explaining that "the Commission's privacy approach evolved to include a focus on specific consumer harms as the primary means of addressing consumer privacy issues").

[222] *See* FTC STAFF, SELF-REGULATORY PRINCIPLES, *supra* note 138, at 6–12 (describing the FTC's efforts to promote self-regulation for online privacy during the 2000s).

[223] FTC, PROTECTING CONSUMER PRIVACY, *supra* note 7.

[224] *Id.* at vii–viii.

notice-and-choice and some commonalities with the Obama administration's 2012 policy paper. For one thing, the report recognizes that it may be counterproductive to offer consumers notice and choice at every opportunity; instead, the FTC proposes the principle that "[c]ompanies should simplify consumer choice."[225] Doing so, the report explains, "increases consumers' control over the collection and use of their data"[226]—that is, less (notice and choice) is sometimes more (beneficial to individual privacy interests). Notice and choice, therefore, are not required—and by the logic of the report's discussion, are discouraged—"before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer."[227] The test is an objective one based on "the consumer's relationship with a business," rather than "the inherently subjective test of consumer expectations."[228] The examples the report offers where notice-and-choice would not be required are similar to those in the Obama Administration policy paper: "[order] fulfilment, fraud prevention, internal operations, legal compliance and public purpose, and most first-party marketing."[229]

If the information is to be used in ways that are inconsistent with the consumer's reasonable expectations, then the FTC wants the company to provide notice, generally prior to collecting the information, and choice about whether it may be collected.[230] In two circumstances, the choice must be opt-in: where the information a company has collected is to be used "in a manner materially different than claimed at the time of collection" and where the information is "sensitive."[231] While offering no general definition of "sensitive," the report adopts the "consensus" view that "information about children, financial and health information, Social Security numbers, and precise geolocation data" falls into this category.[232]

### *B. FIPPs in Positive Law*

Like many statements of principles, the statements of fair information practice principles discussed above might have remained merely theoretical, little affecting the world. But in fact, the principles have been translated into positive law as well as self-regulatory codes of conduct. The following reviews some of the more prominent implementations of FIPPs in positive law, demonstrating that the theoretical problematics of notice-and-choice appear also in the real-world implementations.

---

225 *Id.* at 35.

226 *Id.* at 36. The report notes that simplifying choice also helps information collectors: it "preserves the ability of companies to innovate new products and services." *Id.*

227 *Id.* at 48.

228 *Id.* at 38.

229 *Id.* at 39.

230 *Id.* at 48–50. The report acknowledges that there are circumstances where it would be impractical to provide notice before collection.

231 *Id.* at 57.

232 *Id.* at 59.

### 1. The Privacy Act of 1974

Congress took heed of the recommendations presented in the 1973 HEW Report and enacted some of them as the Privacy Act of 1974.[233] The Act requires federal government agencies[234] to supply three types of notices of their practices that implicate information privacy. The first is a description of any "system of records" that the agency maintains, which the agency must publish in the Federal Register at the time the agency establishes or revises it.[235] This notice implements one of the principles of the HEW Report,[236] but, lacking specifics and being confined to the pages of the Federal Register, does little to facilitate an individual's decision whether to supply his PII.

The second is a notice that an agency must provide to an individual when the agency asks the individual to supply it with information.[237] The notice must state whether the individual's provision of the requested information is "mandatory or voluntary"; the purpose of the information collection; the "routine uses" that may be made of the information; and the effects on the individual of his failure to provide the information.[238] The Act specifies where the notice must appear—it must be "on the form which [the agency] uses to collect the information or on a separate form that can be retained by the individual"—but does not require any particular level of prominence.[239] These provisions embody several of the principles of the HEW Report.[240]

The third type of notice is only implied in the statute,[241] in a provision that forbids an agency to disclose information about an individual without obtaining his "prior

---

[233] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (1988)). Although the HEW report recommended legislation that would apply to both the government and the private sector, the Privacy Act applies only to certain agencies of the federal government. *See infra* note 234. This limitation of its scope resulted from lobbying by industry groups. *See* Thompson, *supra* note 164, at 35. Nevertheless, "the Privacy Act embodies all five principles upon which the Code was based." Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 969 n.89 (1991).

[234] The Act applies principally to agencies of the federal government's executive branch and independent agencies. It does not apply to agencies of state or local governments, 5 U.S.C. § 552a(a)(1) (referencing definition in 5 U.S.C. § 552(e)), except for one provision dealing with use of Social Security numbers, *id.* § 552a note.

[235] *Id.* § 552a(e)(4). An agency maintains a "system of records" if it holds information about individuals that it is able to retrieve by using the individual's name or some identifying number. *Id.* § 552a(a)(5).

[236] *See* HEW REPORT, *supra* note 22, at 41 ("There must be no personal-data record-keeping systems whose very existence is secret.").

[237] 5 U.S.C. § 552a(e)(3).

[238] *Id.* § 552a(e)(3). A "routine use" is defined in the statute as any use "for a purpose which is compatible with the purpose for which it was collected." *Id.* § 552a(a)(7).

[239] *Id.* § 552a(e)(3).

[240] *See supra* text accompanying notes 170–73.

[241] An OMB guidance anticipates that a request for consent will at least state "the general purposes for, or types of recipients, to which disclosure may be made." Responsibilities for the

written consent."[242] The law does not indicate whether opt-out consent is sufficient.[243] While the OMB has stated that "a blanket or open-ended consent" is not adequate,[244] there does not seem to be any determination by a court as to whether opt-out consent suffices. The consent requirement in any event has limited applicability because the statute includes a number of exceptions allowing disclosure without consent.[245] The most capacious of these exceptions is one for a "routine use" of the information.[246]

The data collector need not offer any choice about whether to submit the requested data—the submission requirement may be "mandatory."[247] But this rule effectively is irrelevant because the collector is the ultimate monopoly supplier of services, an agency of the United States government. The agency might just as well declare that the provision of information is "voluntary," adding that if an individual chooses not to supply the information, he will not receive Social Security benefits, a permit allowing him to begin construction of a factory, or various other benefits.

### 2. The EU Data Protection Directive (1995) and General Data Protection Regulation (2016)

The European Union's Data Protection Directive has comprehensively regulated a wide swathe of information practices in the EU since its 1998 effective date.[248] The goal of the legislation was to create a harmonized set of national rules that would protect individual privacy while not unduly interfering with the free flow of information needed for international commerce.[249] Notice and choice are foundational principles. The data collector must notify the data subject of "the purposes of the processing for which the data are intended."[250] Where required for "fair processing" of the data, the collector must also identify "the recipients or categories of recipients of the data" and must disclose "whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply."[251] As a general rule, the data collector is required to obtain the data subject's "unambiguous[]"

---

Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. 28948, 28954 (July 9, 1975).

242 5 U.S.C. § 552a(b). Disclosure is also allowed upon the individual's "written request." *Id.* Such a request, originating from the individual, does not assume any provision of notice by the agency. *See id.*

243 *See id.*

244 Responsibilities for the Maintenance of Records, 40 Fed. Reg. at 28954.

245 5 U.S.C. § 552a(b)(1)–(12).

246 *Id.* § 552a(b)(3).

247 *Id.* § 552a(e)(3)(A).

248 Data Protection Directive, *supra* note 151.

249 *Id.* at Recitals 10, 56 ("the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy," but "cross-border flows of personal data are necessary to the expansion of international trade").

250 *Id.* art. 10(b).

251 *Id.* art. 10(c).

consent before engaging in any "processing"[252] of the data,[253] and "explicit" consent is required before processing specified categories of sensitive data.[254] However, the consent provision is subject to several exceptions that narrow its scope. An inevitable exception exists for uses necessary to complete the transaction, where the individual's consent may be inferred from his act of entering into the transaction.[255] There is also a vague and all-purpose exception where "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."[256]

National implementations of the Data Protection Directive ("Directive") turned out not to be uniform; the Directive requires only a minimum level of privacy protection, allowing member states to implement a higher level of protection, and some member states did just that. Driven largely by the desire to create a uniform, Community-wide set of privacy rules, the EU promulgated the General Data Protection Regulation[257] ("GDPR"), which will go into effect on May 25, 2018.[258] As a regulation, and unlike a directive, the GDPR applies directly throughout the EU, preventing the development of non-uniform versions in different member states. The GDPR differs from the Directive in a variety of respects, but retains the principles of notice and choice. The GDPR specifies additional items of information of which the data subject must be notified before data collection[259] and exhibits some concern that the notice should actually be available to the data subject.[260] Where consent is required, the GDPR requires opt-in consent: consent must be tendered through "a clear affirmative action,"[261] and "[s]ilence, pre-ticked boxes or inactivity should not . . . constitute

---

[252] *Id.* art. 7(a). "Processing" is broadly defined to include any collection, use, or disclosure of data. *Id.* art. 2(b).

[253] An opinion of the Directive's Article 29 Working Party states that this consent must be opt-in, since consent delivered through an opt-out mechanism is not "unambiguous." Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent, 01197/11/EN, WP187 (July 13, 2011), at 21–25.

[254] Data Protection Directive, *supra* note 151, art. 8(2)(a).

[255] *Id.* art. 7(b).

[256] *Id.* art. 7(f). For discussion of these exceptions, see Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 670–71 (2002).

[257] GDPR, *supra* note 151.

[258] *Id.* art. 84(2).

[259] The notice must include contact information of the data collector, state the period of time during which the data will be retained, describe access and withdrawal rights, and (in all circumstances) identify the recipients or categories of recipients of the data. *Id.* art. 13(1), (2).

[260] Notice must be "in a concise, transparent, intelligible and easily accessible form." *Id.* art. 12(1). If the notice is in a format that also deals with other matters, it must be "clearly distinguishable from the other matters." *Id.* art. 7(2).

[261] *Id.* art. 6(1).

consent."[262] As with the Directive, the consent requirement is limited by substantial exceptions.[263]

3. Children's Online Privacy Protection Act (1998)

In 1998, prompted by a recommendation from the FTC, Congress enacted legislation aimed at protecting children's privacy online and charged the FTC with promulgating implementing regulations.[264] Mirroring the requirements of the statute, the FTC's rule requires the operator of a website that is directed to children to post a notice of its privacy practices and to obtain "verifiable parental consent" before collecting personal information from children.[265] The rule is unusually specific in requiring that the notice be presented in a manner that is likely to come to the attention of the child's parent: the notice must be "clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials," and the collector "must make reasonable efforts . . . to ensure that [the] parent . . . receives direct notice."[266] The consent must be tendered through an opt-in mechanism.[267]

4. Gramm-Leach-Bliley Act (1999)

Title V of the Gramm-Leach-Bliley Act ("GLB")[268] requires financial institutions to provide privacy notices and (in some circumstances) opt-out choice to their customers.[269] "Clear and conspicuous" notices are required at the time the institution initially establishes a relationship with the customer and annually thereafter.[270] The notices must describe the categories of nonpublic personal information that the institution collects and discloses as well as the categories of third parties (whether affiliated or nonaffiliated) to which it discloses such information.[271] If the institution

---

[262] *Id.* at Recital 32.

[263] *Id.* art. 6(b)–(f).

[264] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2018).

[265] 16 C.F.R. § 312.3(b) (2018).

[266] *Id.* § 312.4(a), (b). The notice must also be posted on the website. *Id.* § 312.4(d).

[267] *Id.* § 312.5(b). Because children are involved, the consent procedures are unusually stringent and require much more from the parent than clicking a website button. Acceptable methods for a parent to tender consent include sending in a signed consent form by mail or fax; using a credit card to pay for a transaction at the website; calling a telephone number to provide verbal consent; having a videoconference with trained personnel; and providing a government-issued identification. *Id.* § 312.5(b)(2)(i)–(v).

[268] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2018). Regulations issued by the Consumer Financial Protection Bureau implement GLB with respect to most categories of covered financial institutions. The regulations appear at 12 C.F.R. Part 1016, also known as Regulation P.

[269] The regulation makes a distinction between "customer" and "consumers," but for simplicity, I elide that distinction here. 12 C.F.R. § 1016.3(e), (i) (2018).

[270] *Id.* § 1016.4(a), .5(a)(1).

[271] *Id.* § 1016.6(a). "Nonpublic personal information" is defined in the regulation through a complex set of interlocking definitions. *Id.* § 1016.3(p)(1)–(3). Simplified a bit, it consists of information relating to a consumer that the institution obtains in connection with providing

wishes to disclose nonpublic personal information to a nonaffiliated third party, it must include in the notice a disclosure to this effect as well as a reasonable means for the customer to opt out of the disclosure.[272] The institution may make the disclosure only if, after a reasonable opportunity, the customer does not opt out.[273]

GLB notices usually appear as pieces of paper included in a bill or some other mailing from the financial institution.[274] In 2009, the federal agencies that administer GLB published a model disclosure form that financial institutions may use for their GLB notices.[275] Use of the model form acts as a safe harbor, constituting compliance with the disclosure requirements.[276] Probably every reader of this Article is familiar with them—and has seen so many of them that she tosses them into the trash without reading them as she would any form of junk mail. The development of a model form, which is widely used by the financial institutions subject to GLB, makes the notices unusually consumer-friendly.

GLB implements the notice principle more seriously than most implementations. GLB requires "clear and conspicuous" notice, defined as notice that is "reasonably understandable and designed to call attention to the nature and significance of the information in the notice."[277]

5. California Online Privacy Protection Act (2003)

As explained above,[278] in 2000, the FTC announced that self-regulation had failed and recommended that Congress enact legislation requiring all consumer-oriented commercial websites that collect PII "to comply with the four widely-accepted fair

financial services, unless the institution has a reasonable basis for believing that the information is publicly available. *Id.*

[272] There are certain exceptions to the opt-out requirement, such as when the disclosure is made so that the third party can provide services for the institution; to carry out a consumer transaction; or at the customer's request. *Id.* § 1016.13–.15. A "nonaffiliated third party" is, roughly, an entity that is not under common control with the financial institution. *Id.* § 1016.3(a)(1), (o)(1)–(2).

[273] *Id.* § 1016.10. Reasonable means for opting out include via a check-off box, a reply form, an email, a website, or a toll-free telephone number. The customer generally must be allowed thirty days to exercise the opt-out right. *Id.* § 1016.10.

[274] The regulation requires that notices be delivered in such a way that "each consumer can reasonably be expected to receive actual notice in writing." *Id.* § 1016.9(a). Delivery by postal mail is specifically deemed reasonable. *Id.* § 1016.9(b)(ii). Notices may be delivered electronically if the customer agrees. *Id.* § 1016.9(a). A 2014 amendment to Regulation P allows institutions whose practices do not trigger the opt-out requirement to dispense with the annual paper notices and instead inform the consumer on the billing statement that the notice is available on the institution's website. *Id*. § 1016.9(c)(2).

[275] Development of a model form was mandated by a 2006 amendment to GLB, codified at 15 U.S.C. § 6803(e). Fillable model forms are linked from a document titled *Instructions for Using the Privacy Notice Online Form Builder*, FED. RES. (Sept. 3, 2010), http://www.federalreserve.gov/bankinforeg/privacy_notice_instructions.pdf.

[276] 16 U.S.C. § 6803(e)(4) (2018).

[277] 12 C.F.R. § 1016.3(b)(1).

[278] *See supra* text accompanying note 206.

information practices," including notice and choice.[279] Congress did not enact the recommended legislation, but the California legislature heard the call.[280] The California Online Privacy Protection Act of 2003 ("CalOPPA") requires operators of commercial websites that collect PII from California residents to post a privacy policy.[281] The policy must identify the categories of PII that the website collects and the categories of third parties to which it may disclose the PII.[282] The policy also must describe the procedure the website uses to notify website visitors of changes to its privacy policy.[283] The website must post the policy "conspicuously," which may be through placing a link labeled "Privacy" on the website's home page.[284]

In 2010, the *Wall Street Journal* published the results of its examination of 101 popular smartphone apps running on the Android and iPhone platforms.[285] It found that about half of them transmitted the phone's unique identifier to a third party without the user's knowledge or consent, about half transmitted location information, and five transmitted the user's age, gender, and other personal information. Only about half of the apps posted a privacy policy, either within the app or on an associated website.

In 2012, referencing the *Wall Street Journal* report, as well as another study finding that only five percent of mobile apps had a privacy policy,[286] California's Attorney General, Kamala Harris, issued an interpretation of CalOPPA.[287] Harris found that the statute's requirement to post a privacy policy applied not only to websites, but also to mobile apps.[288] At the same time, she announced that she had

---

279 *See* FTC, FAIR INFORMATION PRACTICES, *supra* note 206, at 36.

280 Stats. 2003, c. 829 (A.B. 68), § 3 (codified at CAL. BUS. & PROF. CODE § 22575(a), (b)). A 2013 amendment to the statute requires some additional categories of disclosure: how the website responds to a do-not-track request conveyed via a browser setting and whether the website allows third parties to collect PII across multiple websites. Stats. 2013, c. 390 (A.B. 370), § 1 (codified at CAL. BUS. & PROF. CODE § 22575(b)(5)–(7)).

281 CAL. BUS. & PROF. CODE § 22575(a) (2018).

282 *Id.* § 22575(b)(1).

283 *Id.* § 22575(b)(3).

284 *Id.* § 22577(b)(3).

285 Scott Thurm & Yukari Iwatani Kane, *What They Know: A Wall Street Journal Investigation: Your Apps Are Watching You*, WALL ST. J., Dec. 18, 2010, at C1.

286 Kamala D. Harris, *Mobile Applications and Mobile Privacy Fact Sheet*, https://www.oag.ca.gov/system/files/attachments/press_releases/n2630_updated_mobile_apps_info.pdf.

287 Kamala D. Harris, *Joint Statement of Principles* (Feb. 22, 2012) [hereinafter Harris, *Joint Statement of Principles*], https://www.oag.ca.gov/system/files/attachments/press_releases/n2630_signed_agreement.pdf.

288 *Id.* The relevant language of the statute makes it applicable to "[a]n operator of a commercial Web site or online service that collects personally identifiable information through the Internet." CAL. BUS. & PROF. CODE § 22575(a) (2018). A 2015 Delaware law that generally tracks the language of the California statute is more explicitly expansive in its coverage, applying to "[a]n operator of a commercial internet website, online or cloud computing service, online application, or mobile application that collects personally identifiable information through the Internet." DEL. CODE ANN. tit. 6, § 1205C(a) (2018).

entered into an agreement with Apple, Google, Amazon.com, and other operators of mobile app platforms under which they agreed to require the apps they host to post a privacy policy.[289] The agreement requires the companies to post privacy notices "conspicuously," which may be via clicking on a link from somewhere within the app.[290] Shortly after the agreement was implemented, the percentage of apps posting privacy policies substantially increased.[291] In a staff report, the FTC applauded the California effort and recommended that app platforms require, and app developers include, a privacy notice.[292] Since California residents can access every commercial website and mobile app, this statute effectively has national reach. However, the California law implements the principle of notice, but not that of choice.

6. Federal Communications Commission's Privacy Rules for Internet Service Providers (2016)

The Federal Communications Commission's ("FCC") 2015 network neutrality rule reclassified broadband Internet access service as a "telecommunications service" subject to common-carrier regulation under Title II of the Communications Act.[293] That action removed Internet service providers ("ISPs") from the jurisdiction of the FTC and made the ISPs subject to the FCC's statutory authority to protect the privacy of telecommunications data.[294] The FCC thereafter commenced a rulemaking to establish appropriate protections for "individually identifiable CPNI, personally identifiable information (PII), and content of communications."[295] The FCC issued a

[289] Harris, *Joint Statement of Principles*, *supra* note 287, ¶ 1. Facebook later signed on to the agreement, bringing its App Center within the agreement's scope. Press Release, State of Cal. Dep't of Justice, Attorney General Kamala D. Harris Announces Expansion of California's Consumer Privacy Protections to Social Apps as Facebook Signs Apps Agreement (June 22, 2012), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california%E2%80%99s-consumer.

[290] Harris, *Joint Statement of Principles*, *supra* note 287, ¶ 2.

[291] KAMALA D. HARRIS, ATTORNEY GEN. OF CAL., PRIVACY ON THE GO 4 (2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf. In December 2012, the state of California brought its first enforcement action under CalOPPA, charging that Delta Airlines violated the Act by failing to post a privacy policy in its Fly Delta mobile app. The California Court of Appeal dismissed the action, finding it preempted by the Airline Deregulation Act. People *ex rel*. Harris v. Delta Air Lines, Inc., 247 Cal. App. 4th 884 (Cal. Ct. App. 2016).

[292] FED. TRADE COMM'N STAFF, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY i–iii, 12 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[293] Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601 (2015), *abrogated by* Restoring Internet Freedom, 2018 WL 305638 (F.C.C. 2018). For an explanation of the tortuous path leading to issuance of this order, see John A. Rothchild, *Understanding Network Neutrality*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW, *supra* note 219, at 419.

[294] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911 (2016), ¶¶ 24, 26 [hereinafter FCC, ISP Privacy Rules].

[295] *Id.* ¶ 46. CPNI stands for "customer proprietary network information" and consists of telecommunications metadata, analogous to what the 1995 NTIA white paper refers to as "TRPI." *See supra* text accompanying note 185.

final rule on October 27, 2016.[296] On the heels of the national elections of November 2016, which gave Republicans control of both branches of Congress as well as the presidency, Congress nullified this rule before it became effective by exercising its powers under the Congressional Review Act.[297]

The FCC's rules on notice and choice closely track those in the 2012 FTC report and the 2015 discussion draft of the Consumer Privacy Bill of Rights Act.[298] An ISP must provide its customers with notice of the types of personal information it collects, how it uses that information, how it discloses the information to third parties, and what privacy choices the customer has.[299] The notice must be made available by a "clear and conspicuous" link that appears both on the home page of the carrier's website and on any mobile app that the carrier provides consumers for account management purposes.[300] Additionally, the notice must "provide information in language that is comprehensible and not misleading."[301]

Customers must be given choice, which may be via an opt-out mechanism, as to whether their personal information may be used or disclosed for purposes other than providing telecommunications service.[302] As in the FTC's recommendation, opt-in consent is required before the ISP may use or share sensitive information[303] or use PII in a manner inconsistent with the privacy policy in effect at the time it was collected.[304] Opt-out consent is adequate in other situations.[305]

### *C. FIPPs in Voluntary Implementations*

Several self-regulatory schemes addressing online privacy are based on the FIPPs. The resulting rules are, unsurprisingly, founded upon notice-and-choice.

---

296 FCC, ISP Privacy Rules, *supra* note 294.

297 S.J. Res. 34, 115th Cong., 131 Stat. 88 (2017). Cecilia Kang, *Congress Moves to Overturn Obama-Era Online Privacy Rules*, N.Y. TIMES (Mar. 28, 2017), https://www.nytimes.com/2017/03/28/technology/congress-votes-to-overturn-obama-era-online-privacy-rules.html. On May 18, 2017, Rep. Marsha Blackburn (R-TN) introduced a bill that would reinstate by statute the principal provisions of the FCC's rules. Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, H.R. 2520, 115th Cong. (2017).

298 FCC, ISP Privacy Rules, *supra* note 294, ¶ 9 ("In adopting rules governing customer choice, we look to the best practices framework recommended by the FTC in its 2012 Privacy Report as well as the choice framework in the Administration's CPBR . . . .").

299 *Id.* ¶ 126.

300 *Id.* ¶¶ 140–41.

301 *Id.* ¶ 144.

302 *Id.* ¶¶ 132, 196.

303 *Id.* ¶ 172. The FCC's list of what counts as "sensitive" information is slightly broader than the FTC's. *Id.* ¶ 177.

304 *Id.* ¶ 195 (requiring opt-in consent to "material retroactive changes to privacy policies").

305 *Id.* ¶ 196 (requiring "opt-out approval to use, disclose, or permit access to non-sensitive customer PI").

1. Website Privacy Policies (Ca. 1995 to Date)

During its first foray into online privacy, the FTC used its bully pulpit to urge online sellers to post a privacy policy on their website. The FTC's efforts commenced with a public hearing in June 1996.[306] The December 1996 staff report on the meeting noted that workshop participants generally were in agreement that the principles of notice and choice—whose origins it traced to the 1973 HEW Report—should govern online privacy.[307] However, at the time the report was written, "few Web sites [had] privacy policies or display[ed] their information practices to consumers."[308] Industry members "recogniz[ed] the need to address this issue," but industry members and privacy advocates disagreed on how to implement the fair information practice principles.[309] Industry members were in favor of allowing self-regulation to flower, while privacy advocates called for some level of regulatory engagement by the government.[310] The report took no position on whether the online industry should be allowed more time to regulate itself by implementing the principles of notice and choice.[311]

Despite the report's inconclusive outcome, the workshop had the effect of galvanizing industry participants into self-regulatory action. Two industry associations, the Interactive Services Association and the Direct Marketing Association, announced at the workshop itself that they were releasing self-regulatory guidelines for protecting online privacy. The guidelines say that commercial websites should post a privacy policy and honor a narrow category of opt-out requests.[312] The following month, a nonprofit organization called TRUSTe announced the launch of its online privacy seal program, which allowed a website that met TRUSTe's requirements to display the TRUSTe seal.[313]

---

[306] FED. TRADE COMM'N STAFF, PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE 2 (1996), https://www.ftc.gov/reports/staff-report-public-workshop-consumer-privacy-global-information-infrastructure.

[307] *Id.* The FTC had held some earlier hearings and workshops addressing online privacy in 1995. *Id.* at 1–2, nn.1–2.

[308] *Id.* at 8.

[309] *Id.* at 8–11.

[310] *Id.* at 26–29.

[311] *Id.* at 51 (noting opposing views but not taking a position).

[312] Press Release, Interactive Services Association, Interactive Services Association Issues Positions on Privacy and Online Marketing (June 4, 1996). The two associations' appended Joint Statement on Online Notice and Opt-Out called for "[a]ll marketers operating online sites" to post a notice describing their collection and use of personal information from site visitors, and to furnish them "with the opportunity to request that their e-mail addresses not be rented, sold, or exchanged for online solicitation purposes." *Id.*

[313] *eTRUST Launches Pilot Program*, ELEC. FRONTIER FOUND. (Dec. 20, 1996), https://www.eff.org/effector/9/15. The organization was originally named eTRUST but was rechristened TRUSTe due to a trademark conflict. In June 2017, its name was changed to TrustArc. Chris Babel, *TRUSTe Transforms to TrustArc*, TRUSTARC (June 6, 2017), http://www.trustarc.com/blog/2017/06/06/truste-transforms-to-trustarc/. As of this writing, the privacy seals continue to be branded as TRUSTe.

In 2009, a group of advertising and marketing trade associations (later dubbed the Digital Advertising Alliance ("DAA")) responded to an FTC staff report by issuing a self-regulatory framework applying to online behavioral advertising ("OBA").[314] The framework includes elements of notice and choice that place obligations on operators of websites through which information is collected for the purpose of OBA as well as on companies that engage in OBA or facilitate it (including advertising networks). OBA is defined as collecting data from multiple websites to enable companies (other than the collecting website itself) to target advertising based on predicted user preferences derived from the data.[315] A website that allows information to be collected for OBA purposes must deploy a link (separate from the "Privacy" link) that goes directly to a website maintained by the DAA.[316] The website provides information about OBA and allows the user to opt out of the collection and use of her information for OBA. The link may be labeled with text such as "Interest-Based Ads" or consist of an icon (▷) designed for this purpose.[317] The DAA website includes a "partial list" of a few hundred companies that participate in the framework.[318] The Advertising Self-Regulatory Council enforces compliance with the framework through its Online Interest-Based Advertising Accountability Program ("Accountability Program").[319] The Accountability Program has rendered decisions in more than seventy enforcement actions since 2011.[320] As a result of some recent challenges, Budweiser added an icon link to the DAA opt-out page on its website,[321] and Wayfair added a link labeled "Interest-Based Ads" on its website.[322]

At present, finding a consumer-oriented commercial website of any substantial size that does not post a privacy policy would be challenging. These policies generally

---

[314] *See* AM. ASS'N OF ADVERT. AGENCIES ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 29 (2009), http://www.aboutads.info/obaprinciples (noting that the principles "are informed by" the FTC staff document of the same name); FTC STAFF, SELF-REGULATORY PRINCIPLES, *supra* note 138, at 45–47 (FTC staff's version of the principles).

[315] AM. ASS'N OF ADVERT. AGENCIES ET AL., *supra* note 314, at 10–11 (defining "online behavioral advertising"); *id.* at 23–24 (elucidating that definition).

[316] *Webchoices: Digital Advertising Alliance's Consumer Choice Tool for Web (Beta)*, DIGITAL ADVERT. ALLIANCE, http://www.aboutads.info/choices/ (last visited Feb. 10, 2018).

[317] This description simplifies a fairly complex regulatory scheme, which also involves notices by the third parties that actually do the collecting and by service providers, alternative means of complying with the requirements, and other features.

[318] *DAA Participating Companies & Organizations*, DIGITAL ADVERT. ALLIANCE, http://digitaladvertisingalliance.org/participating (last visited Feb. 10, 2018).

[319] The Advertising Self-Regulatory Council is a unit of the Council of Better Business Bureaus, one of the founding members of the DAA. *ASRC Snapshot*, ASRC, http://www.asrcreviews.org/about-us/ (last visited Feb. 10, 2018).

[320] The decisions are available at *Accountability Program Decisions, Dispositions, Closures, and Guidance*, ASRC, http://www.asrcreviews.org/accountability-program-decisions/ (last visited Feb. 10, 2018).

[321] Anheuser-Busch Companies, Case No. 70-2017 (Online Interest-Based Advertising Accountability Program Jan. 25, 2017).

[322] Wayfair Inc., Case No. 71-2017 (Online Interest-Based Advertising Accountability Program Jan. 25, 2017).

implement the principles of notice and choice in some manner. Those relatively few[323] websites that display a TRUSTe privacy seal must conform to TRUSTe's rules. These rules currently require (1) notice that discloses fifteen specified categories of information and (2) opt-in choice before sharing PII in a manner not consistent with the privacy notice, before sharing any of a defined set of "sensitive information," and before using PII that is collected from a source other than the data subject for a purpose beyond that for which it was collected.[324] The vast majority of websites, which post a privacy policy but do not participate in TRUSTe's program, are subject only to the minimal notice requirements of CalOPPA.[325]

2. Mobile App Privacy Policies and Permissions (Ca. 2008 to Date)

As discussed above, in 2012 California's Attorney General found that the 2003 CalOPPA requires mobile apps to post a privacy policy. Both the Apple App Store and the Google Play Store, agreeing to abide by that interpretation, implement the California rules in developer guidelines, with some variations.[326] Both require apps that collect PII to post a privacy policy—the minimum required by California law as interpreted by the Attorney General. Both also require user consent under certain circumstances before collection and disclosure.[327] Apple goes beyond these procedural rules and includes a few substantive ones: apps may not require submission of personal data except where needed for "core functionality" of the app; data may not be shared with third parties except to improve user experience and for approved advertising; data acquired via the HomeKit API may not be used for advertising; data from Apple Pay may not be shared with third parties except to facilitate delivery of goods or services; and there are limitations on the sharing of health information.[328]

Privacy in mobile apps is also controlled through the use of permissions. Once downloaded to a user's mobile device, an app may request permission to access various types of personal information that resides on or may be acquired through the device, as well as to access certain hardware functions. On the Android 6.0 platform,

---

[323] TrustArc itself claims to have "more than 1,000" clients. *Why TrustArc*, TRUSTARC, https://www.trustarc.com/why-trustarc/ (last visited Feb. 10, 2018). There are over a billion websites out there. *Total Number of Websites*, INTERNET LIVE STATS, http://www.internetlivestats.com/total-number-of-websites/ (last visited Feb. 10, 2018).

[324] *Enterprise Privacy Certification Standards*, TRUSTE, https://www.truste.com/privacy-certification-standards/ (last visited Feb. 10, 2018).

[325] *See supra* text accompanying notes 281–84.

[326] *App Store Review Guidelines*, APPLE, https://developer.apple.com/app-store/review/guidelines/ (last visited May 2, 2017); *Let's Build the World's Most Trusted Source for Apps and Games*, GOOGLE, https://play.google.com/about/developer-content-policy-print/ (last visited May 17, 2017).

[327] Apple states: "Apps that collect user or usage data must have a privacy policy and secure user consent for the collection. . . . [Apps cannot] use or transmit someone's personal data without first obtaining their permission and providing access to information about how and where the data will be used." APPLE, *supra* note 326, at 5.1.1(i), 5.1.2(i). Google states: "If your app collects and transmits personal or sensitive user data unrelated to functionality . . . then prior to the collection and transmission, it must prominently highlight how the user data will be used and have the user provide affirmative consent for such use." GOOGLE, *supra* note 326.

[328] APPLE, *supra* note 326, at 5.1.1(ii), 5.1.2(ii)–(iv), 5.1.3(i).

apps may request permission to access body sensors, calendar, camera, contacts, location, microphone, phone, SMS, and storage.[329] Granting any of these permissions can give access to highly personal information.[330] Permission is not granted by default, but only via an opt-in mechanism. Under Android 6.0 (but not under earlier versions), the user may grant some but not all of the requested permissions and may later revoke the grant of a permission.[331] Nevertheless, some of the choices made available via setting permissions are actually required; if the user denies permission, the app will not function correctly. A phone app, for example, will not function if permission to access the microphone is denied.

In addition, the DAA has extended its self-regulatory framework so that it applies to mobile apps.[332] The publisher of an app that allows third parties to collect "cross-app data" (that is, data from multiple apps on a particular device) must post a link to a disclosure that the user will see either before downloading it from the app supplier platform, when the app is opened for the first time, or when cross-app data is collected.[333] The link must also be available in the app's settings.[334] The disclosure must offer the user the ability to opt out of the collection of such data.[335] If the app allows third parties to collect "precise location data," then similar notice rules apply and the app must seek prior opt-in consent from the user.[336]

---

[329] *Google Play Help*, GOOGLE, https://support.google.com/googleplay/answer/6270602 (last visited Feb. 10, 2018). Each of these permissions is actually the name of a "permission group" that may contain one or more individual permissions. Chris Hoffman, *How to Manage App Permissions on Android*, HOW TO GEEK (June 8, 2017), https://www.howtogeek.com/230683/how-to-manage-app-permissions-on-android-6.0/. The user cannot control the individual permissions within a permission group. *Id.*

[330] However, it is often difficult to know how personal the disclosed information will be. For example, if you grant an app the Location permission group, the app may use the "access approximate location" function to determine your location to within a few thousand meters, or it may use the "access precise location" function, which uses GPS to determine your location within a few meters. *Google Maps Help*, GOOGLE, https://support.google.com/maps/answer/2839911?co=GENIE.Platform%3DAndroid&hl=en (last visited Feb. 10, 2018). You might not mind if an app knows what neighborhood you are in, but might mind very much if it knows what building you are in.

[331] Under versions of Android earlier than 6.0, permission had to be granted on an all-or-none basis. KENNETH OLMSTEAD & MICHELLE ATKINSON, PEW RESEARCH CTR., APP PERMISSIONS IN THE GOOGLE PLAY STORE 9 (2015), http://www.pewinternet.org/files/2015/11/PI_2015-11-10_apps-permissions_FINAL.pdf. The Apple iOS has long allowed individualized grant or denial of permissions. Chris Hoffman, *iOS Has App Permissions, Too: And They're Arguably Better Than Android's*, HOW TO GEEK (Dec. 15, 2013), https://www.howtogeek.com/177711/ios-has-app-permissions-too-and-theyre-arguably-better-than-androids/.

[332] DIGITAL ADVERTISING ALLIANCE, APPLICATION OF SELF-REGULATORY PRINCIPLES TO THE MOBILE ENVIRONMENT 1 (2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf.

[333] *Id.* at 15.

[334] *Id.*

[335] *Id.* at 17.

[336] *Id.* at 21–28.

The framework bans the collection and use of information for certain purposes—eligibility for employment, credit, health care treatment, and insurance[337]—and restricts the collection and use of "sensitive data," including "financial account numbers, Social Security numbers, pharmaceutical prescriptions, [and] medical records."[338] In some recent enforcement actions, SEGA solved its problem by removing third-party collection of data for OBA from its Sonic Runners app,[339] and iTriage agreed to add links to its disclosures in its pages in the app download platforms and to stop authorizing the collection of precise location data.[340]

Thus, in the mobile app ecosystem, an unusual amalgam of rules governs privacy: California state law, which has been effectively federalized due to the infeasibility and undesirability of blocking users located in California; an industry-devised self-regulatory framework; and platform operators going beyond legal requirements by incorporating an element of choice.

3. IoT Privacy Policies (Ca. 2011 to Date)

Currently, no established voluntary regime of privacy notices exists for IoT devices. An unscientific sampling of the websites that manufacturers use to showcase their IoT devices reveals that the great majority of them do not offer any information about how private information acquired by the device is handled, even while expatiating on the device's other functions.

Application of the notice-and-choice paradigm to IoT devices has an obstacle to overcome beyond those that plague websites and mobile apps. Unlike the large visual displays attached to computers, the medium-sized ones built into tablets, and the small but usable displays of smartphones, most IoT devices lack a visual interface that is capable of displaying the quantity of information contained in a privacy policy. Therefore, conveying notice, and receiving consent, are problematic. There are workarounds. For example, privacy notice-and-choice could be part of a setup routine that the user must follow using one of his other connected devices. The privacy policy could be printed on a piece of paper in the device's box along with a statement explaining that, by using the device, the consumer is deemed to have consented to the described privacy practices—by analogy with the "shrinkwrap" licenses and "money now, terms later"[341] approaches that were heavily debated in the early days of electronic commerce—or a practice of including the device's privacy policy on the manufacturer's website could take hold. However, the workarounds all suffer from various weaknesses.[342]

---

337 *Id.* at 31–32.

338 *Id.* at 32. As with the discussion of the DAA's Online Behavioral Advertising Principles, *supra* note 317, this discussion simplifies a complex scheme.

339 SEGA, Case No. 65-2016 (Online Interest-Based Advertising Accountability Program July 14, 2016).

340 iTriage LLC, Case No. 64-2016 (Online Interest-Based Advertising Accountability Program July 14, 2016).

341 ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996).

342 *See* Sara Shahmiri, *Wearing Your Data on Your Sleeve: Wearables, the FTC, and the Privacy Implications of This New Technology*, 18 TEX. REV. ENT. & SPORTS L. 25, 29–30 (2016).

Such IoT privacy policies as are available pre-purchase indicate that IoT privacy policies may closely resemble website privacy policies. For example, if you install a Wi-Fi-connected refrigerator, oven, or dishwasher from GE Appliances, the company will collect information including "[r]eal-time usage information for your connected Appliances, such as the number of times a door of a connected Appliance is opened, the type and/or number of cycles run by a connected Appliance and the date your connected Appliance was installed" as well as "[l]ocation data of your connected Appliance based upon your connected Appliance's IP address, MAC address, RFID and/or WiFi connection."[343] With your "prior consent"—the notice does not specify whether the choice mechanism is opt-in or opt-out—the company will also track the location of the mobile phone that you use to control the appliance.[344] GE Appliances may use the collected information for its own marketing purposes and may share the information "with third parties that may offer you products or services for purposes related to your purchase and use of a GE Appliances WiFi Connect Appliance (e.g., certified service providers)."[345]

Another example comes from Philips, a manufacturer of connected light bulbs. If you install the bulbs, the manufacturer will learn the geolocation of the bulbs, the names you assign to each room in your house in which a bulb is located, and information about your movements within the house as collected by a motion sensor.[346]

If you go to Amazon's website to purchase an Echo and want to know the device's privacy policy before you buy, you will be disappointed. The policy is not easy to find. Starting from the Echo product page,[347] you have to scroll down to the section titled "Technical details," spot the sentence that reads "Use of the Amazon Echo is subject to the terms found here," click on the word "here," which links to a page titled "Alexa and Alexa Device Terms," click on a link labeled "Alexa Terms of Use," and scroll down to paragraph "3.1 Information."[348] There you learn that Alexa collects information from you that Amazon will handle "in accordance with the Amazon.com

---

[343] *Connected Data Privacy Policy*, GE APPLIANCES (June 6, 2016), http://www.geappliances.com/privacy/privacy_policy_connected.htm.

[344] *Id.*

[345] *Id.*; *see* Transcript of Hearing, Federal Trade Commission: Internet of Things Workshop (Nov. 19, 2013), at 59 (statement of Michael Beyerle, Marketing Manager for Innovation at GE Appliances) ("The wi-fi router system is feeding into the GE servers, the GE server allowing you to connect into your smart phone, your tablet, whatever device you may have, as well as some data storage.").

[346] *Privacy Notice for Hue*, PHILIPS (Mar. 1, 2017), http://www2.meethue.com/en-us/privacy-policy/. Some users may find solace in the privacy policy's assurance that "[w]e do not use this data to monitor you and make sure third parties with access to this data agree not to either." *Id.*

[347] *Echo (2nd Generation)*, AMAZON, https://www.amazon.com/all-new-amazon-echo-speaker-with-wifi-alexa-dark-charcoal/dp/B06XCM9LJ4/ref=sr_tr_sr_1 (last visited Mar. 7, 2018).

[348] *Alexa Terms of Use*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740 (last updated Dec. 6, 2017).

Privacy Notice."[349] That privacy notice says nothing specific to Alexa.[350] The general statement about sharing information with third parties suggests that Amazon may send whatever information it captures from your use of Alexa to third parties if you fail to respond to an opt-out notice: "Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information."[351] The Google Home website likewise offers no privacy policy for the device itself.[352]

## IV. WHY THE NOTICE-AND-CHOICE PARADIGM CANNOT EFFECTIVELY REGULATE THE COLLECTION AND USE OF PII IN THE ONLINE ECOSYSTEM

Notice-and-choice, as set out in the leading formulations of fair information practice principles and as implemented in positive law and in voluntary systems of self-regulation, has failed as a paradigm for regulating the collection and use of private information in the online commercial ecosystem. It has failed because it does not, and cannot, accomplish the fundamental goal of a privacy regime, namely that of empowering individuals to exercise control over the use of their personal information.

In this Section, I begin by explaining how we should judge whether a system for regulating online privacy is successful. I go on to discuss reasons why notice-and-choice is for fundamental reasons incapable of achieving this goal.

First, the notice-and-choice paradigm is internally inconsistent because it requires data subjects, who it assumes are rational economic beings, to behave irrationally. Second, the notice element of notice-and-choice, as it appears in both statements and implementations of FIPPs, fails to meet accepted standards for adequacy that apply in the related contexts of contracting and consumer protection and cannot feasibly be reformed to meet those standards. Third, notice-and-choice amounts to blanket consent due to the non-transactional nature of privacy interactions. Blanket consent is not appropriately applied to privacy connected with Internet-enabled data flows because consumers cannot anticipate the uses that will be made of their private data. Fourth, notice-and-choice cannot work when PII is transferred to a third party for uses that are not disclosed and could not be disclosed because not known to the transferor. A data collector cannot provide notice of, or seek consent for, third-party uses of the data that the collector itself is unable to anticipate. Fifth, notice-and-choice cannot work with some types of IoT devices because third parties are not in a position to consent to the collection of data about them.

### *A. Criteria for Evaluating a Regime that Regulates Online Privacy*

Determining whether notice-and-choice is an appropriate framework for protecting privacy in the context of websites, mobile apps, and the IoT first requires that we have a criterion for success. I posit that *a privacy framework can be deemed successful only if, in practice, it allows consumers a meaningful opportunity to decide whether to share their personal information*. Stated negatively, a framework is a

---

349 *Id.*

350 *See Amazon Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 (last updated Sept. 30, 2016).

351 *Id.*

352 *See Google Home*, GOOGLE STORE, https://store.google.com/product/google_home (last visited Jan. 27, 2018).

failure if it presents consumers with merely formal choices that are not choices in reality. I will not devote much effort to justifying this position, as it simply restates the essence of what we mean when we speak of information privacy, inherent in the accepted understanding of the term.[353]

It is one thing to be offered a choice. It is another to have a meaningful opportunity to exercise a choice that one is offered. Whether a meaningful choice is available in a given situation is harder to determine than might initially appear. Systems of notice-and-choice generally do not grapple with this problem, assuming instead that choice is a bivalent property of a situation—one is either presented with a choice or not. A simple example illustrates the difficulty. If a person points a gun at you and says, "Your money or your life," you may in one sense be said to have exercised choice when you select the former, but the maker of the offer could not successfully defend her right to keep the money on the ground that, after all, you chose to tender it as the best of the available options. If we apply a more realistic concept of "choice," one that recognizes that the availability of choice is a matter of degree, it becomes clear that in most situations involving Internet-enabled data flows, the consumer is not presented with anything that could rightly be considered a choice.

In such contexts, a choice about the disposition of one's private information may be merely formal, and therefore not actual, for several reasons. First, *a choice is not actually available if the chooser is not aware of it*. Each of the statements of the FIPPs discussed above calls for the data collector to provide notice of its practices concerning collection and use of personal information. Yet, none of them states the basic principle that notice should be so designed as to reach the attention of a reasonable data subject. A few of these statements evince some awareness of the issue in recognizing that complex or unneeded notices may be counterproductive,[354] but fail to call for conspicuous placement of the notice.

Implementations of the notice principle in positive law and voluntary practices fare little better on this score. The Privacy Act allows notice of routine uses to be supplied separately from the form used to solicit the data[355] and does not specify how notice of

---

[353] Consider some of the leading definitions of the term "information privacy": (1) "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." WESTIN, *supra* note 19, at 7; (2) One of the "core principles" of privacy is "to ensure to the greatest possible extent individual awareness, participation and control" over personal data. OECD, PRIVACY FRAMEWORK, *supra* note 178, at 41 (quotation is from the Explanatory Memorandum that accompanies the Guidelines); (3) Several "noteworthy" formulations of the concept of privacy include "that the data subject should decide the nature and extent" of disclosure of data concerning him. HEW REPORT, *supra* note 22, at 39–40.

[354] *See* WHITE HOUSE, *supra* note 167, at 16–17 (no need for "prominent notice" of data practices that will be obvious to the data subject); FTC, PROTECTING CONSUMER PRIVACY, *supra* note 7, at 64 ("Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.").

[355] *See supra* text accompanying note 239. Allowing the notice to be separated from the collecting instrument can severely interfere with the conveyance of actual notice. For example, the Privacy Act notice for the familiar IRS Form 1040, the U.S Individual Income Tax Return, appears not on the form itself but on page 100 of the 107-page instruction booklet that may be consulted when filling out the form. Form 1040 itself vaguely references this notice with a line at the bottom of its first page: "For Disclosure, Privacy Act, and Paperwork Reduction Act Notice, see separate instructions." IRS, FORM 1040, U.S. INDIVIDUAL INCOME TAX RETURN (2017). Anecdotal evidence suggests that few users of the form spot the reference or the Privacy

disclosure is to be conveyed.[356] The EU Data Protection Directive does not specify how entities should convey notice.[357] The EU GDPR states some requirements for the notice that sound good—notice must be "concise, transparent, intelligible and easily accessible"[358]—but that would seem to be satisfied by a notice that is clearly written and available via a single click but unlikely to come to the data subject's attention.

The FCC's ISP rules allow notice to be banished to a location that is accessible only if the customer clicks on a link on the ISP's website.[359] CalOPPA requires privacy notices to be posted "conspicuously," but defines this term to include an inconspicuous placement accessed by clicking on a "Privacy" hyperlink on the website's home page (or, in the case of a mobile app, from somewhere within the app).[360] The DAA mechanism that allows a consumer to opt out from collection and use of her personal information for online behavioral advertising is visible only if one clicks on another such link.[361]

GLB notices are probably the best of the bunch. They usually follow a standardized, consumer-friendly format and are delivered to consumers on a piece of paper included with a bill or other mailing once a year.[362] Nevertheless, some evidence suggests that consumers rarely read the notices.[363] This probably corresponds to the experience of most readers of this Article, despite their being unusually skilled in comprehending legal texts.

The absence of notice that is likely to come to the attention of the data subject vitiates the possibility of real choice. An individual's decision to participate in a transaction that results in the collection of her PII cannot with any semblance of reality be construed as an exercise of her consent to that collection of information if she did not receive notice that her participation in the transaction would result in the information collection. The failure of the FIPPs and implementations of them to

---

Act notice on page 100 of the booklet. This renders effectively unavailable to users of Form 1040 a piece of information that the Act requires be conveyed: you, the filer, "do not have to provide your daytime phone number" in the box that requests it. IRS, 1040 INSTRUCTIONS (2017).

356 *See supra* text accompanying note 242.

357 Article 10 of the Directive simply states that the controller "must provide a data subject" with specified information. Data Protection Directive, *supra* note 151, art. 10.

358 GDPR, *supra* note 151, art. 12(1).

359 *See supra* text accompanying note 300.

360 *See supra* text accompanying notes 284, 290.

361 *See supra* text accompanying note 316.

362 *See supra* text accompanying note 274.

363 *See* Eric Poggemiller, Note, *The Consumer Response to Privacy Provisions in Gramm-Leach-Bliley: Much Ado About Nothing?*, 6 N.C. BANKING INST. 617, 632 (2002) (reporting assessments that "many people had not 'looked twice' at their privacy notices and were not even sure what they were" and "consumers are 'sick of them . . . . They think it's junk mail and it goes straight to the circular file.'"); Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P), 79 Fed. Reg. 64057, 64059 (Oct. 28, 2014) (noting financial industry commenters' statement that "most customers ignore annual privacy notices").

require conveyance of actual notice means that individuals are not exercising choice over the disposition of their personal information.

Second, *gun-to-the-head choice is not actual choice*. Several of the FIPPs formulations discussed above, and two of the implementations of notice-and-choice in positive law, recognize that the chooser in the gun-to-the-head scenario mentioned above is not exercising real choice and identify scenarios involving Internet-enabled data flows that present an analogous, if lesser, degree of coercion.

- Although the point did not make its way into the report itself, the discussions of the committee that produced the 1973 HEW Report did raise it. One speaker at a committee meeting focused on inequalities in bargaining power.[364] A person who applies for a job, for which he has a great need, is in no position to exercise a choice about whether to hand over whatever personal information the prospective employer demands: "The individual is anxious to get the job and the employer says, well now . . . I have to know about this, this, this, and that. The individual is really in an imperfect bargaining situation. He is in no position to counter the claims of his prospective employer."[365] Similar points were made repeatedly during the committee's discussion.[366]
- In its 1977 report, the Privacy Protection Study Commission ("PPSC") similarly noted: "When an individual must choose between signing an authorization form and foregoing employment or insurance or public assistance, one cannot realistically speak of his signing voluntarily."[367]

---

[364] Transcript of Proceedings, Secretary's Advisory Committee on Automated Personal Data Systems 43 (May 19, 1972) (Kenneth A. McLean, Professional Staff Member, Committee on Banking, Housing, and Urban Affairs, U.S. Senate). Transcripts of meetings of the Advisory Committee are available at https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/archive-of-the-meetings-of-the-secretarys-advisory-committee-on-automated-personal-data-systems-sacapds/.

[365] *Id.*

[366] *See id.* at 194–95 (a person applying for a benefit from the government experiences "coercion" to supply the required personal information) (Frances Grommers, Visiting Lecturer, Harvard School of Public Health); Transcript of Proceedings, Secretary's Advisory Committee on Automated Personal Data Systems 52–53 (June 15, 1972) (a person applying for Social Security benefits is not in a position to perform a cost-benefit analysis and decide whether to surrender the required personal information) (Joseph Weizenbaum, Professor of Computer Science, MIT); *id.* at 138 ("There is virtually no information that the university obtains that can't be forced out of the students somehow as a condition of registering for the institution . . . .") (Michael A. Lithen, Legal Counsel, University of Wisconsin); Transcript of Proceedings, Secretary's Advisory Committee on Automated Personal Data Systems 25 (July 24, 1972) ("If you condition receiving of black lung benefits on the release of this information, then for all intents and purposes the individual doesn't really have a choice about exchange of data.") (J. Taylor DeWeese).

[367] PRIVACY PROTECTION STUDY COMM'N, *supra* note 175, at 291; *see also id.* at 14 ("[I]n a society in which time is often at a premium, in which organizations performing similar functions tend to ask similar questions, and in which organizational record-keeping practices and the differences among them are poorly perceived or understood, the individual often has little real opportunity to pick and choose.").

- The 1995 NTIA white paper discusses an example of merely formal choice in the context of telecommunications metadata. It explains that when a data collector collects PII (such as a subscriber's telephone number) to provide a particular service (to connect the call) and seeks consent to use that PII for purposes other than providing the service, the data collector may be tempted to condition delivery of the service on the data subject's consent to the ancillary use. An example is a privacy policy that states: "You must consent to our sharing your personal information with our business partners for marketing purposes, or we will not connect your calls." The white paper observes that this proposition deprives consumers of "a meaningful opportunity to accept or reject the terms offered." This is especially the case "in those service markets dominated by a single supplier."[368]
- The FTC's rule implementing the 1998 COPPA says that the operator of a website "is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity."[369] In other words, it prohibits conditioning the provision of a service upon the disclosure of private information that is not needed to complete the requested transaction.
- In its 2012 report, the FTC identifies the characteristics of a situation that offers merely formal choice—what it calls "take it or leave it" choice.[370] It references "the purchase of an important product that has few substitutes, such as a patented medical device."[371] If the seller "offered a limited warranty for the device only in exchange for the consumer's agreeing to disclose his or her income, religion, and other highly-personal information," this would be a violation of fair information principles because "the consumer would not have been offered a meaningful choice."[372] As another example, the FTC points to broadband Internet access service: where there are few alternative suppliers, "the service provider should not condition the provision of broadband on the customer's agreeing to, for example, allow the service provider to track all of the customer's online activity for marketing purposes."[373] On the other hand, in the case of "less

368 NTIA, PRIVACY, *supra* note 184, at 23.

369 16 C.F.R. § 312.7 (2018).

370 FTC, PROTECTING CONSUMER PRIVACY, *supra* note 7, at 51. I find this terminology misleading. In almost all mass-market transactions, the terms are "take-it-or-leave-it" in the sense that there is no bargaining: if a prospective purchaser does not like one of the terms of the product as offered (price, warranty, return policy, etc.), her only options are to accept the terms or walk away from the offer. It is not surprising, or troubling, that no bargaining is permitted over the privacy term. What *is* troubling, as I discuss in text, is when a (non-negotiable) privacy term requires the purchaser to "consent" to collection or use of her private information for purposes extraneous to provision of the purchased good or service.

371 *Id.* at 52.

372 *Id.*

373 *Id.*

important products and services in markets with sufficient alternatives," the FTC considers it acceptable for the vendor to require the consumer's consent to use of her private information for purposes extraneous to the transaction as long as it provides appropriate notice, such as "we provide you with free content in exchange for collecting information about the websites you visit and using it to market products to you."[374]

- The FCC's 2016 privacy rules prohibit broadband Internet access service providers "from conditioning the provision of broadband service on a customer surrendering his or her privacy rights" and "from terminating service or otherwise refusing to provide [Internet access] due to a customer's refusal to waive any such privacy rights. By design, such 'take-it-or-leave-it' practices offer no choice to consumers."[375] The FCC has elsewhere recognized that consumers have few options in selecting a broadband Internet access service; as of 2013, forty-five percent of households had only a single option.[376]
- Finally, the EU's 2016 GDPR expresses disapproval of, without actually prohibiting, the practice of requiring consent to a use of data that is unrelated to the transaction in which the data is collected. The applicable language is: "When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[377]

The upshot of these distinctions between real or meaningful choice and merely formal choice may be formulated as: *If a consumer is offered a good or service, but only on condition that he give up private information that is not required for provision of that good or service, and there are no close substitutes available to the consumer that do* not *require the relinquishment of private information, then the purported choice is in reality no choice at all*. In my view, this states a reasonable criterion for determining whether a particular situation presents a consumer with a meaningful choice that could be deemed to satisfy the choice element of the notice-and-choice principle.

### *B. Why Notice-and-Choice Cannot Satisfy These Criteria*

For the following reasons, the notice-and-choice paradigm does not, and cannot, meet these minimum requirements for an acceptable regulation of privacy in the context of Internet-enabled data flows.

---

374 *Id.*

375 FCC, ISP Privacy Rules, *supra* note 294, ¶ 295.

376 Rothchild, *supra* note 293, at 438.

377 GDPR, *supra* note 151, art. 7(4).

### 1. The Notice-and-Choice Paradigm Presumes that Consumers Are Rational but Requires Them to Behave Irrationally

The premise of notice-and-choice is simple and familiar. Individuals value their privacy, and therefore they have an interest in controlling the disposition of their personal information, an interest that society recognizes as worthy of protection. The notice-and-choice paradigm assumes that individuals act rationally to promote their interests. The paradigm is premised on an application of rational choice theory, according to which individuals can assess the costs and benefits of giving up control over their personal information as well as make rational choices that best promote their own interests and also "guide the marketplace to some acceptable balance between consumer and business interests" with regard to the collection and use of personal information.[378]

This is not to say that a rational individual seeks to minimize the disclosure of her personal information, with the ultimate goal of preventing any such disclosure. To the contrary, there are many situations in which it is rational to disclose personal information in the expectation of receiving something more valuable in exchange. The everyday experience of life in contemporary society makes this clear. To purchase a good via the Internet and have it delivered to her home, a consumer must divulge her name, address, and credit card number. To obtain access to a website, she may have to provide an email address at which a retailer can contact her. To download an app from the Google Play Store or the Apple App Store, she must divulge her mobile telephone number.

#### *a. The Information We Need to Rationally Regulate Disclosure of Our Private Information*

The individual, then, optimizes her utility by relinquishing her privacy just so far as she expects a countervailing benefit of equal or greater value. To make this calculation, she needs information of several types.

First, she needs to know what types of private information the company she is considering doing business with will collect from her. She might be unperturbed if the company gathers and retains her name, address, phone number, and credit card number in the course of a transaction. But she might feel differently if she knows the company is recording every click she makes on a website, keeping a close record of the geographical location of her mobile device, or maintaining in perpetuity every word she speaks into a voice-controlled device.

Second, she needs to know what the company intends to do with her data. A range of possibilities exist. (1) The company might use her data for no other purpose than to perform the transaction that she seeks, thereafter discarding it. (2) The company might add her data to other information that it holds about her, draw inferences about her interests, and use those inferences to target advertising at her. (3) The company might share the information with its affiliated companies that are engaged in some other line of business or (4) with unaffiliated companies, either directly or through advertising networks, again for the purpose of targeted marketing. (5) The company might supply the information to entities that will use it in ways that may constrain her options, such as with health- or life-insurance companies, prospective employers, credit bureaus, the lawyer for her estranged spouse, or government agencies. (6) The company might

[378] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 148 (2016).

share her private information with another entity that has poor security practices, resulting in an intruder gaining access to the information.

Third, she must know the costs she will incur because of the particular uses that the company or its transferees will make of her private information. Referring to the types of sharing listed in the previous paragraph, she would certainly view type one as imposing no costs. She might view type two as costless, but alternatively might believe that it imposes significant costs (for example, if she ordered something personal or embarrassing from a company and then received advertisements for similar products that displayed on her computer monitor in a way that was visible to co-workers or family members). She is more likely to experience costs from type three sharing, and still more from type four. Types five and six will, by definition, impose costs—higher insurance rates, loss of desired employment, paying more for credit, a divorce with less satisfactory terms, being subject to additional screening at airport security, or dealing with the aftermath of identity theft.

Fourth, on the benefit side of the equation, she must know the value to her of the goods or services that she receives by engaging in interactions that result in disclosure of her personal information. The benefits might involve the ability to purchase a good or service, access to information made available via a website, use of an app to play a game or receive turn-by-turn driving instructions, use of a search engine, the ability to adjust her home thermostat while away from home—a list that may be extended endlessly by anyone who makes use of digital networked communications.

*b. What It Would Take to Acquire that Information*

The notice-and-choice paradigm assumes that an individual will use the information conveyed by the statement of an entity's privacy practices ("notice") combined with information gained from other sources to decide rationally whether to allow disclosure of her PII in a particular context ("choice"). The obstacles to achieving this happy outcome are numerous and intractable.

i. Categories One and Two.

Consider the first two categories of information that are necessary for adequate notice: what types of personal information the company will collect and what uses it will make of the PII. Acquiring the information contained in a privacy policy is not a cost-free endeavor. Reading a privacy policy takes time, and time is worth something to a rational person. In economic terms, one incurs an opportunity cost[379] when he spends time doing one thing and therefore forgoes spending the time doing something else. That cost might be easily quantifiable if, for example, the alternative to reading a privacy policy is to spend additional time working at a job for which one is paid an hourly rate. More generally, the opportunity cost is difficult to quantify, as when the alternative is to engage in some form of leisure activity that is more pleasant than reading a privacy policy. Scholars have made attempts to quantify the cost of reading privacy policies. According to one study, it would take the average person 244 hours to read the privacy policies of each website she visits in a year, implying an average

[379] An "opportunity cost" is "that value that is given up or sacrificed in order to secure the higher value that selection of the chosen object embodies." THE NEW PALGRAVE DICTIONARY OF ECONOMICS 719 (John Eatwell et al. eds., 1987).

opportunity cost of $3,534 per person annually.[380] The more recent shift to mobile devices can only increase these costs because for most people (over a certain age), the need to read a lengthy text on the small screen of a smartphone makes the procedure all the more time-consuming.

IoT devices present even greater difficulties. If you see a device in a store or on a website and want to view the privacy policy before buying it, good luck. You could try pulling up the privacy policy from the manufacturer's website, but the chances of finding the device's privacy policy there are slim.[381] That means you will only see the privacy policy once you purchase the device and set it up. Privacy policies typically state that they may be updated from time to time and thus recommend checking back periodically to see if something is new. So, reading the privacy policy associated with an IoT device at the time you purchase or install it is not sufficient; to have up-to-date notice of what the device's manufacturer is doing with your personal information, you need to keep checking back.

Regardless of how much time we spend poring over website privacy policies, we likely will fail to understand them. One study found significant differences in the interpretation of privacy policies within and between groups of expert and non-expert study participants, concluding that the findings "cast doubt on whether website notices, as they are typically worded today, can effectively convey privacy policies to the general public."[382]

The costs of assessing privacy practices do not end there. Before one can decide whether to do business with a company that has a given set of privacy practices, she must know what the alternatives are. If another supplier of the good or service offers a more consumer-friendly privacy policy then, all else being equal, she should prefer that supplier. The only way to learn about the alternative privacy policies is to read them, incurring additional costs.

Despite the time and effort involved, a consumer might find reading and understanding a particular privacy policy worthwhile if it governs a large swathe of her PII. This might be the case if she makes frequent use of social media, such as Facebook or Snapchat, and is concerned enough about what will happen to her private information that she decides to learn about the site's privacy policies (notice) and settings (choice). Similarly, a consumer using an always-on IoT device, like the Amazon Echo or a baby monitor, may also have enough concern about her private information to read and understand the privacy policy.

---

[380] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 563 (2008); *see also* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., BIG DATA AND PRIVACY xii (2014) ("The conceptual problem with notice and consent is that it fundamentally places the burden of privacy protection on the individual . . . . The provider offers a complex, take-it-or-leave-it set of terms, while the user, in practice, can allocate only a few seconds to evaluating the offer."); SOLOVE, THE DIGITAL PERSON, *supra* note 147, at 84 ("There are too many collectors of information for a right of opt-out to be effective. Without a centralized mechanism for individuals to opt-out, individuals would have to spend much of their time guarding their privacy like a hawk.").

[381] *See infra* text following Table 2.

[382] Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 83 (2015).

ii. Category Three.

Once she is aware of the relevant privacy policies, the rational individual must proceed to determine what costs she will incur if she agrees to allow access to her PII in accordance with an information collector's privacy policy. In the vast majority of situations that online consumers are likely to face, this is an impossible task.

To make this calculation of costs, the rational consumer would have to be able to answer at least the following questions.

First, who precisely will gain access to the PII? Except in the relatively rare situations in which the information collector declares (credibly) that it will never disclose PII to anyone else,[383] privacy policies are vague about what other entities will gain access to a user's data. The policies may refer to "affiliates" or "third parties," but almost never specify the parties by name. Even if you knew who would receive data from the information collector, you could not know to whom the recipients would transfer it onward. Any data that leaves the confines of the collecting entity is liable to end up in the hands of data brokers. At that point, you have no way of knowing how your private information will be used and what impacts that use may have on you.[384]

Second, what conclusions about the user will the data yield up when tortured? Modern data analytics techniques, when applied to large data sets, are capable of drawing surprisingly accurate conclusions about individuals.

A few years ago, the Target chain of stores developed a method for identifying its customers who were likely to be pregnant. The goal was to send these customers special offers for baby-related products with the hope that the offers would condition them to shop at Target for items that they would not otherwise associate with that store once the baby arrived. To get a jump on the competition, Target wanted to identify these future consumers of baby items before the information became public through a birth announcement. Using its massive database of customer purchasing data, it

---

383 Even then, issues may arise if the company finds itself in bankruptcy proceedings and its trove of PII becomes an asset of the estate that may be sold to the highest bidder. In several such cases, consumer advocates have objected to the sale on the ground that it would violate the company's privacy policy. For example, when RadioShack was in bankruptcy proceedings, the company proposed to sell its customer information, despite the fact that the company's privacy policy stated: "We will not sell or rent your personally identifiable information to anyone at any time." An FTC official objected to the sale unless stringent conditions were attached. Letter from Jessica Rich, Dir. of the Bureau of Consumer Protection, to Elise Frejka, Esq. (May 16, 2015), https://www.ftc.gov/public-statements/2015/05/letter-jessica-rich-director-bureau-consumer-protection-bankruptcy-court. A group of state attorneys general likewise objected. The sale went through anyway, with some limitations on what data was transferred: telephone numbers were excluded, as were email addresses that had not been active within the previous two years and multiple other categories of personal information. Laura Northrup, *RadioShack Will Not Be Selling Your Phone Number to New Owners*, CONSUMERIST (May 20, 2015), https://consumerist.com/2015/05/20/radioshack-will-not-be-selling-your-phone-number-to-new-owners/. The privacy policies of most of the most highly-trafficked commercial websites now state that personal information may be transferred to a third party in case of sale or bankruptcy. Natasha Singer & Jeremy B. Merrill, *When a Company Is Put Up for Sale, in Many Cases, Your Personal Data Is, Too*, N.Y. TIMES (June 28, 2015), https://nyti.ms/1C04MnG.

384 James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 62 (2003) ("Since it is impossible to know where our information will end up and how it will be used, it is difficult to assess the risks associated with giving out the information or failing to monitor its use once we have released it.").

identified about twenty-five products (such as unscented hand lotion, vitamin supplements, cotton balls, and hand sanitizers) that, when bought in combination, tended to predict that the purchaser was pregnant. Following this method, it sent coupons for baby clothes and cribs to one of its female customers, who happened to be an unmarried high-school student. The girl's father stormed into a Minneapolis-area Target store, demanded to speak with the manager, and expressed outrage. A few days later the father, having learned that his daughter was in fact pregnant, offered his apologies to the store manager.[385]

As discussed above, the set of postings that a Facebook user "Likes" is enormously revealing,[386] as is the home electricity usage that a smart meter captures.[387] We simply cannot know—cannot even imagine—what conclusions advanced data analytics will draw from the mass of personal data that we generate through our online activity.

A third question the consumer must answer is, what impact will this revealed information have on me? The result of all this disclosure might be no worse than receiving coupons in the mail or advertisements in app banner ads for products in which one has no interest. On the other hand, disclosure might lead to paying a higher price for insurance or a denial of employment or credit.[388] There is no way to estimate the likelihood that consenting to a particular release of data may lead to such harms.

A fourth question is whether the recipients of the data will keep it safe from intruders. Security breaches can lead to identity theft, in which the thief obtains a credit card in the victim's name or intercepts the victim's income tax refund. An individual simply cannot calculate the chances that the PII she allows a reputable business to collect may end up in the hands of identity thieves.

iii. Category Four.

The last category of information that our would-be rational consumer needs is what benefits she will receive from allowing access to her personal data. The nature of the benefits will usually be known to her. She will get to purchase a product online, access information made available via a website, download and use an app on her mobile device, or remotely control a connected device. However, she also needs to place a monetary value on the benefits. To do this, she needs to know not merely whether she gains more benefit from the transaction than the monetary cost to her (which may be zero, as when she is offered "free" access to a website or app and her payment consists of the private information that she gives up in the process), but also *how much more benefit* she will get, so she can compare that benefit with the privacy harms that she expects to suffer.

---

385 Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. For further discussion of data analytics techniques, see Shaun B. Spencer, *Predictive Analytics, Consumer Privacy, and Ecommerce Regulation*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW, *supra* note 219, at 492–517.

386 Youyou et al., *supra* note 45.

387 *See supra* text accompanying notes 128–31.

388 *See* GARFINKEL, *supra* note 167, at 22–23 (referencing discussions of the problem of data inaccuracy from the 1960s). Congressional hearings into the problem led to the enactment of the Fair Credit Reporting Act in 1971. *Id.* at 23; *see also* SOLOVE, THE DIGITAL PERSON, *supra* note 147, at 46 ("Not only are our digital biographies reductive, but they are often inaccurate.").

*c. It Would Be Irrational to Engage in this Much Rationality*

Will a rational consumer engage in this four-stage inquiry to decide on a situation-by-situation basis whether to allow access to her personal information? Analyzing the matter from the standpoint of "rational inattention" theory strongly suggests that attempting to do this would be irrational.

The theory of rational inattention results from an application of the common-sense notion that "when information is costly to acquire, decision makers may sometimes choose to act on incomplete information rather than incur the cost to become perfectly informed"—and that the decision to forgo additional efforts to acquire better information is a rational one.[389] This notion is an implication of our "bounded rationality": the fact that humans face limitations in the time they have available to gather information and in their cognitive abilities to process the information in order to arrive at a utility-maximizing decision.[390] Because of these limitations, humans must often rely on heuristics—rules of thumb—when making decisions.[391]

Conversely, it would be irrational—that is, non-welfare-maximizing—for a person to make a decision only after gathering all of the available information bearing on the decision, regardless of the cost to acquire that information. More stringently, rationality demands that one cease acquiring more information when the marginal cost of obtaining the information exceeds the marginal benefit from having it. Any policy that fails to recognize the constraints imposed by the fact of bounded rationality is a misguided one.

Several factors determine how much information a rational person should acquire before making a decision in a given situation.[392] First, the greater the cost of acquiring additional information in comparison with the potential gains that may accrue if the additional information leads to a welfare-enhancing decision, the more likely that forgoing the acquisition of that information will be rational. If it is expensive for the consumer to acquire better information about what uses a data collector will make of his PII, how those uses will impact him, and what he will gain by giving up the PII, in relation to the harms that he might avoid if he makes a better-informed decision, then forgoing the additional information is more likely to be rational. If, on the other hand, acquiring additional information is relatively cheap, then the effort of acquiring the information more likely will pay off.

Ordinary experience tells us that acquiring information about the privacy practices of the companies we may choose to interact with via the Web, mobile apps, and IoT

---

[389] James M. Sallee, *Rational Inattention and Energy Efficiency*, 57 J.L. & ECON. 781, 781 (2014).

[390] "The term 'bounded rationality' is used to designate rational choice that takes into account the cognitive limitations of the decision-maker—limitations of both knowledge and computational capacity." THE NEW PALGRAVE DICTIONARY OF ECONOMICS, *supra* note 379, at 266.

[391] Rational inattention is related to the concept of "satisficing": "choos[ing] an alternative that meets or exceeds specified criteria, but that is not guaranteed to be either unique or in any sense the best." *Id.* at 243. It is rational to be content with a satisfactory option, rather than expending additional effort to find the best option, if the cost of obtaining the additional information needed to optimize exceeds the expected gains therefrom.

[392] The following discussion of these factors is adapted, with some significant modifications, from Sallee, *supra* note 389, at 782–83.

devices is expensive. Privacy policies are difficult to read and, for persons of ordinary sensibilities, provide little or no amusement value. The study referenced above indicates that the time one would need to spend reading the privacy policies that one encounters in typical interactions with the Internet is large in comparison with other major uses of time.[393] The 244-hours-a-year estimate that appears in that study amounts to the number of hours in six forty-hour work weeks, or about twelve percent of a work year. But that time spent is only the start. The amount of time and effort that would be required to determine what entities will receive your private information, what uses they will make of that information through combining it with other data and applying data analytics, and the expected value of the resulting harms to you is beyond calculation. Solid information on these matters just is not available.

The second factor to consider is the extent to which the additional information will reduce uncertainty. If the additional information available at a reasonable cost would not do much to alleviate the uncertainty relative to the decision that must be made, gathering the additional information is less likely to pay off. The potential benefit from additional information comes from an enhanced ability to calculate the costs or benefits associated with a particular option. If the new information does not reduce the uncertainty much, the benefits of acquiring it will be correspondingly less.

Gathering additional information can reduce some elements of uncertainty relevant to deciding whether to expose one's personal information. In particular, reading privacy policies can reduce uncertainty about what uses the information collector will make of PII and what sorts of third parties might come into possession of it. But reading privacy policies does little to reduce the amount of uncertainty about the impact uses of PII by the information collector and any transferees will have on the data subject. Reducing uncertainty requires predicting future conduct by a large number of third parties whose identities can only be guessed at. A data analytics company might take the PII the consumer released; combine it with private information about him already in the hands of other information collectors and with publically available information; perform state-of-the-art analytics on the entire corpus of data; derive certain inferences that cast him in a negative light; and provide those inferences to a prospective employer.[394] That employer may decide on the basis of those inferences not to offer him a position, with the result that he is relegated to less desirable employment.[395] A data broker might sell his information to a scam artist who will try to separate him from some of his cash[396] or might handle his information carelessly, leading to unauthorized access and identity theft or other harms.[397] Because

[393] *See supra* text accompanying note 380.

[394] *See* PAM DIXON & ROBERT GELLMAN, THE SCORING OF AMERICA 73–74 (2014), http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf.

[395] *Id.* at 73–75 (describing a situation in which a marketing executive was denied a job because his Klout score, created by applying a secret algorithm to his social media postings, was too low).

[396] Charles Duhigg, *Firms Sell Elderly Americans' Data to Telemarketing Con Artists*, N.Y. TIMES (May 21, 2007), www.nytimes.com/2007/05/21/world/americas/21iht-data.1.5803543.html (describing telemarketing scam aimed at elderly people whom data broker identified as "gullible").

[397] Numerous lawsuits have been predicated on identity theft resulting from unauthorized access to data collected through online interactions. *See, e.g.*, Order Granting Preliminary

the inferences that data brokers derive from the information may be erroneous, the harms that the inferences create may be unjustified.[398]

On the other hand, the release of an individual's PII might have no negative effects on him at all, or might even have a positive effect, such as bringing him to the attention of another prospective employer who otherwise would not have recruited him or causing him to receive a well-targeted advertisement that leads to a desirable product or discount.

Because of this wide spectrum of potential impacts, ranging from the very harmful to the mildly beneficial, gathering additional information at the time when a consumer is deciding whether to enter a transaction that involves exposure of some private information can do little to sharpen his estimate of the expected impact of that exposure on his welfare.

A third factor that the rational consumer must consider is the set of alternatives at her disposal. A dearth of alternatives that one might select based on additional information makes it less likely that gathering additional information will pay off. The whole point of gathering the information is to be able to exercise a more informed choice. If few alternatives are available, the extra information will not help much.

The question is whether, if we do not like a particular vendor's privacy practices, we can choose to obtain a reasonably close substitute from another source that offers a more favorable privacy policy. A review of privacy policies applying to websites, mobile apps, and IoT devices suggests that this condition is not met.

Table 1. Disclosure of Privacy Practices in Website Privacy Notices.[399]

| | Uses Cookies | Uses Web Bugs | Collects Unique Device Identifier | Allows Advertising Networks to Collect PII | Collects Location | Third Parties Use PII to Send Targeted Ads | Collects or Uses PII to Send Targeted Ads |
|---|---|---|---|---|---|---|---|
| Amazon.com[400] | X | X | X | X | X | X | X |
| Walmart.com[401] | X | X | X | X | X | X | X |

Approval of Settlement, Directing Notice to the Class, Scheduling a Final Approval Hearing, and Certifying a Settlement Class, *In re* Ashley Madison Customer Data Security Breach Litig., No. 4:15-MD–02669–JAR (E.D. Mo. July 21, 2017) (approving $11.2 million settlement of class action based on data breach from AshleyMadison.com); *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015) (holding that customers whose personal information was accessed in security breach at Zappos.com lacked Article III standing based on increased risk of identity theft).

398 *See* Adam Tanner, *Data Brokers Don't Know You from a Naked Man Stumbling on the Beach*, FORBES (Aug. 6, 2013), https://www.forbes.com/sites/adamtanner/2013/08/06/data-brokers-dont-know-you-from-a-naked-man-stumbling-on-the-beach/ (discussing errors in information held by data brokers).

399 Further information supporting the conclusions drawn in this Table is on file with the author.

400 *See Amazon Privacy Notice*, AMAZON, *supra* note 350.

401 *See Walmart Privacy Policy*, WALMART, https://corporate.walmart.com/privacy-security/walmart-privacy-policy (last updated Nov. 2017).

| | Uses Cookies | Uses Web Bugs | Collects Unique Device Identifier | Allows Advertising Networks to Collect PII | Collects Location | Third Parties Use PII to Send Targeted Ads | Collects or Uses PII to Send Targeted Ads |
|---|---|---|---|---|---|---|---|
| Google.com[402] | X | X | X | X | X | X | X |
| YouTube.com[403] | X | X | X | X | X | X | X |
| Facebook.com[404] | X | X | X | X | X | X | X |
| Twitter.com[405] | X | X | X | X | X | X | X |
| eBay.com[406] | X | X | X | X | X | X | X |
| Yahoo.com[407] | X | X | X | X | X | X | X |
| Reddit.com[408] | X | X | X | X | X | X | X |
| Yelp.com[409] | X | X | X | X | X | X | X |
| BuzzFeed.com[410] | X | X | X | X | X | X | X |
| Adobe.com[411] | X | X | X | X | X | X | X |
| Bing.com[412] | X | X | X | X | X | X | X |
| LinkedIn.com[413] | X | X | X | X | X | X | X |

[402] *See Google Privacy Policy*, GOOGLE, https://www.google.com/policies/privacy/ (last updated Dec. 18, 2017).

[403] *See id.*

[404] *See Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last updated Sept. 29, 2016); *About Facebook Ads*, FACEBOOK, https://www.facebook.com/about/ads/ (last visited Mar. 10, 2018).

[405] *See Twitter Privacy Policy*, TWITTER (June 18, 2017), https://twitter.com/en/privacy; *Twitter's Use of Cookies and Similar Technologies*, https://help.twitter.com/en/rules-and-policies/twitter-cookies (last visited Mar. 10, 2018).

[406] *See Privacy Policy*, EBAY (Nov. 16, 2015), https://www.ebayinc.com/privacy-policy/.

[407] *See Privacy Policy*, YAHOO!, https://policies.yahoo.com/in/en/yahoo/privacy/index.htm (last updated June 13, 2017).

[408] *See Reddit, Inc. Privacy Policy*, REDDIT (Dec. 12, 2017), https://www.reddit.com/help/privacypolicy/; *Reddit Privacy Policy*, REDDIT (Apr. 10, 2015), https://www.reddit.com/help/privacypolicy/?v=a9aa089a-dfb1-11e4-b70a-22000bc14708.

[409] *See Privacy Policy*, YELP, https://www.yelp.com/tos/privacy_en_us_20160131 (last updated Jan. 31, 2016).

[410] *See Legal at BuzzFeed: Privacy Policy*, BUZZFEED (Feb. 16, 2017), https://www.buzzfeed.com/about/privacy.

[411] *See Adobe Privacy Policy*, ADOBE, https://www.adobe.com/privacy/policy.html (last updated May 29, 2017).

[412] *See Microsoft Privacy Statement*, MICROSOFT, https://privacy.microsoft.com/en-us/privacystatement (last updated Feb. 2018).

[413] *See Privacy Policy: Your Privacy Matters*, LINKEDIN (June 7, 2017), https://www.linkedin.com/legal/privacy-policy.

| | Uses Cookies | Uses Web Bugs | Collects Unique Device Identifier | Allows Advertising Networks to Collect PII | Collects Location | Third Parties Use PII to Send Targeted Ads | Collects or Uses PII to Send Targeted Ads |
|---|---|---|---|---|---|---|---|
| Live.com[414] | X | X | X | X | X | X | X |
| Pinterest.com[415] | X | X | X | X | X | X | X |
| Netflix.com[416] | X | X | X | X | X | X | X |
| Wikia.com[417] | X | X | X | X | X | X | X |
| Craigslist.com[418] | X | X | | | X | | |
| Tumblr.com[419] | X | X | X | X | X | X | X |
| NYTimes.com[420] | X | X | X | X | X | X | X |
| UrbanDictionary.com[421] | X | X | X | X | X | X | X |
| ESPN.com[422] | X | X | X | X | X | X | X |
| TripAdvisor.com[423] | X | X | | X | X | X | X |
| Apple.com[424] | X | X | X | X | X | | X |
| Totals | 25 | 25 | 23 | 24 | 25 | 23 | 24 |

Table 1 summarizes the principal notice-and-choice elements of the privacy policies posted on the twenty-five most-visited commercial websites.[425] An "X"

414 *See Microsoft Privacy Statement*, MICROSOFT, *supra* note 412.

415 *See Privacy Policy*, PINTEREST (Nov. 1, 2016), https://policy.pinterest.com/en/privacy-policy.

416 *See Privacy Statement*, NETFLIX, https://help.netflix.com/legal/privacy (last updated Nov. 30, 2016).

417 *See Privacy Policy*, WIKIA, http://www.wikia.com/Privacy_Policy (last updated July 2017).

418 *See Craigslist Privacy Policy*, CRAIGSLIST, https://www.craigslist.org/about/privacy.policy (last updated July 9, 2015).

419 *See Privacy Policy*, TUMBLR, https://www.tumblr.com/policy/en/privacy (last updated June 13, 2017).

420 *See Privacy Policy*, N.Y. TIMES, https://help.nytimes.com/hc/en-us/articles/115014892108-Privacy-policy (last updated Oct. 27, 2017).

421 *See Privacy Policy*, URBAN DICTIONARY, http://about.urbandictionary.com/privacy (last updated Nov. 2008).

422 *See Privacy Policy*, WALT DISNEY CO., https://privacy.thewaltdisneycompany.com/en/ (last updated Oct. 16, 2017).

423 *See Media Center: Privacy Policy*, TRIPADVISOR, https://tripadvisor.mediaroom.com/us-privacy-policy (last visited Jan. 21, 2018).

424 *See Privacy Policy*, APPLE, https://www.apple.com/legal/privacy/en-ww/ (last updated Jan. 19, 2018).

425 The selection of the twenty-five websites was based on a listing posted by Quantcast, in August 2017, slightly modified to exclude sites that are not commercial (Wikipedia.org) or that provide only a platform (Wordpress.com). *Top Websites*, QUANTCAST,

indicates that the indicated provision was present in the privacy policy. The policies display remarkable uniformity:

- All twenty-five of the websites use cookies and web bugs to collect information from site visitors and store that information in a manner that links it to the computer the visitor used and, generally, to the individual who uses the computer.
- Twenty-three of the twenty-five websites collect a unique identifier attached to the user's computing device, making it impossible to maintain anonymity by refusing or deleting cookies.
- Twenty-four of the twenty-five websites allow advertising networks to collect the user's information.
- All twenty-five of the websites collect the user's location.
- Twenty-three of the twenty-five websites share user data with third parties, generally to permit targeted advertising.
- Twenty-four of the twenty-five websites use the individual's data to send her targeted ads for the site's own products.

Some survey evidence reflects this uniformity. A consumer survey conducted in 2015 indicated that many consumers have felt compelled to deal with an online supplier, even though they lacked confidence in the supplier's privacy practices, due to lack of any alternatives.[426]

https://www.quantcast.com/top-sites/US (last visited Jan. 21, 2018). Privacy policies are not always written very clearly, so in some cases I had to guess at the meaning or make simplifying assumptions.

The methodology of the survey is vulnerable to the criticism that what is really needed is a comparison among the privacy policies of suppliers of goods that are substitutes for each other, rather than those of the most popular websites, which generally occupy different market segments. That sort of survey is not practical within this scope of this Article. For present purposes, I think it is a reasonable assumption that other sellers within a market sector will tend to emulate the market leaders with respect to privacy practices.

[426] TRUSTe, *Study Finds More Americans Concerned About Privacy Than Losing Their Income*, PR NEWSWIRE (Jan. 28, 2016), https://www.prnewswire.com/news-releases/study-finds-more-americans-concerned-about-data-privacy-than-losing-their-income-300211216.html ("Interestingly 19 percent said they continued to use a website they didn't trust to handle their personal information responsibly, with 31 percent of those who reported doing this saying it was because it was the only website that sold a particular product or service.").

Table 2. Disclosure of Privacy Practices in Mobile App Privacy Notices.[427]

| | Uses Cookies | Uses Web Bugs | Collects Unique Device Identifier | Allows Advertising Networks to Collect PII | Collects Location | Third Parties Use PII to Send Targeted Ads | Collector Uses PII to Send Targeted Ads |
|---|---|---|---|---|---|---|---|
| Messenger[428] | X | X | X | X | X | X | X |
| Facebook[429] | X | X | X | X | X | X | X |
| Instagram[430] | X | X | X | X | X | X | X |
| Snapchat[431] | X | X | X | X | X | X | X |
| Netflix[432] | X | X | X | X | X | X | X |
| Spotify[433] | X | X | X | X | X | X | X |
| WhatsApp[434] | X | | X | X | X | | X |
| Uber[435] | X | X | X | X | X | X | X |
| YouTube[436] | X | X | X | X | X | X | X |
| Google Maps[437] | X | X | X | X | X | X | X |
| Totals | 10 | 9 | 10 | 10 | 10 | 9 | 10 |

Table 2 summarizes the findings of a review of the top ten mobile apps.[438] An "X" indicates that the indicated provision was present in the privacy policy. One can find the privacy policies for these apps by going to the app's page in the Google Play Store or Apple App Store and tapping on "Privacy Policy." For all of these apps, tapping on

[427] Further information supporting the conclusions drawn in this Table is on file with the author.

[428] *See Data Policy*, FACEBOOK, *supra* note 404.

[429] *See id.*

[430] *See Privacy Policy*, INSTAGRAM, https://help.instagram.com/155833707900388 (last updated Jan. 19, 2013).

[431] *See Privacy Policy*, SNAP INC., https://www.snap.com/en-US/privacy/privacy-policy/ (last updated Apr. 19, 2018).

[432] *See Privacy Statement*, NETFLIX, *supra* note 416.

[433] *See Privacy Policy*, SPOTIFY, https://www.spotify.com/us/legal/privacy-policy/ (last updated Sept. 9, 2015).

[434] *See WhatsApp Privacy Policy*, WHATSAPP, https://www.whatsapp.com/legal/#privacy-policy/ (last updated Aug. 25, 2016).

[435] *See Privacy Policy*, UBER, https://privacy.uber.com/policy (last updated Sept. 21, 2017).

[436] *See Google Privacy Policy*, GOOGLE, *supra* note 402.

[437] *See id.*

[438] This list is derived from a ranking of apps for the first quarter of 2017. Oliver Yeh, *Top Apps of Q1 2017: Netflix Dominated Worldwide Revenue, Which Grew 63% YoY*, SENSOR TOWER (Apr. 17, 2017), https://sensortower.com/blog/top-apps-q1-2017.

this link brings up the privacy policy of the associated website—none of them offers a privacy policy that is specific to the app. As a result, the privacy policies for the apps are about as uniform as those for websites discussed above:

- All ten of the apps use cookies, and nine use web bugs to collect usage information.
- All ten of the apps collect a unique identifier attached to the user's mobile device.
- All ten of the apps allow advertising networks to collect the user's information.
- All ten of the apps collect the user's location.
- Nine out of ten apps share the user's data with third parties for targeted advertising.
- All ten of the apps use collected data to send users targeted advertisements for the app developer's own products.

It is difficult to collect information about the privacy policies of IoT devices. Based on my own sampling, most manufacturers of the devices do not make the device's privacy policy available on a website. Of the twenty-four IoT devices mentioned above, only ten have a privacy policy available on the manufacturer's website, and several of these are only minimally informative. My sampling of IoT devices offered on the shelves of my local Best Buy store did not turn up any devices that include the privacy policy on the outside of the device's box or on any nearby display. A practice of disclosing the privacy policy of IoT devices pre-purchase may yet develop. Regardless, whether the manufacturers will converge on a common set of privacy terms remains to be seen.

The uniformity among privacy policies applying to websites, mobile apps, and (perhaps) IoT devices calls to mind the uniformity among the sets of contract terms posted by ecommerce websites.[439] The mechanism in the two realms is similar and not difficult to divine. Because, as discussed above, rational consumers do not read and comprehend privacy policies any more than they do online contract terms, no business has any incentive to implement (contract or privacy) terms that are more pro-consumer if doing so entails any costs. And such terms generally do entail costs. For instance, an online business that omits a mandatory arbitration clause from its Terms and Conditions would incur greater litigation costs but would not get much more revenue in return. That same business, should it pledge in its privacy policy not to use its customers' private information for targeted advertising, would lose a source of revenue but would not gain much offsetting revenue from grateful customers.

The absence of any significant competition with respect to privacy policies shows that the long-running debate between opt-in and opt-out choice mechanisms is a red herring. Privacy advocates generally take the position that only opt-in choice reflects

[439] *See* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 41–42 (2013). Radin supposes, reasonably enough, that the terms appearing in contractual boilerplate resemble each other because the firms copy each other's terms. *Id.* at 41. In earlier times, similarity in contract terms proposed by competing sellers may have resulted from the use of standardized paper contract forms. *See* O'Callaghan v. Waller & Beckwith Realty Co., 155 N.E.2d 545, 548 (Ill. 1958) (Bristow, J., dissenting) (referencing clauses that "were included in all form leases used by practically all landlords in urban areas").

a true exercise of the data subject's choice,[440] on the ground that the failure to opt out is an equivocal action. Failure to opt out may reflect the data subject's decision to allow the data collection in question; or it may simply mean that the data subject was not aware of the opportunity to opt out because the notice did not reach her or she chose not to invest the effort required to determine whether to allow the information collection. Accordingly, many privacy advocates consider that choice exercised through an opt-out mechanism is choice in name only—merely formal choice.

Entities that have an interest in collecting PII, on the other hand, generally favor opt-out.[441] They argue that most data subjects are indifferent about whether their PII is collected and how it is used. Because of that indifference, few people will make the effort to opt into a data collection. Therefore, the argument goes, inferring approval from non-action more accurately reflects consumer preferences than inferring non-approval.

But if no real choice exists, the difference between opt-in and opt-out evaporates. Regardless of the choice mechanism, a consumer's options are either to accept the industry-standard privacy-invasive practices or stay off the Internet. To repurpose a classic anecdote about a Hobson's Choice, if all Model T automobiles are painted black, the consumer's choice of color is no more meaningful if exercised through an opt-in mechanism (being required to check a box next to the color she wants, with the only option being ☐ Black) than an opt-out mechanism (if you don't want black, leave this dealership and don't come back).[442]

Fourth, if the amount of utility that an individual can expect to gain by choosing a vendor with a more favorable privacy policy is small compared to the possible loss she would incur by obtaining the good or service from a different vendor with a more favorable privacy policy, then investing in additional information is less likely to pay off. The loss in this context could consist of purchasing the same good from a different vendor at a higher price or making do with a vendor whose non-privacy-related features are less desirable. The underlying idea is that the provider's privacy policy is a feature of the product that, like any of its physical attributes, will affect the consumer's evaluation of the product. In this respect, the seller's privacy policy is analogous to the warranty that the seller includes with the product; all else being equal, a consumer will prefer a product with a longer or stronger warranty, and likewise will

---

[440] *See, e.g.*, Comments of the Electronic Privacy Information Center 15 (May 27, 2016), Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 ("[O]pt-out regimes make it difficult for consumers to exercise their preference not to disclose personal information to others."); Joseph A. Tomain, *Online Privacy & the First Amendment: An Opt-In Approach to Data Processing*, 83 U. CIN. L. REV. 1, 24–26 (2014); Letter from Advocacy Organizations to Senate Commerce Committee (Aug. 9, 2000), https://epic.org/privacy/internet/NAI_group_letter.html (criticizing opt-out as "burdensome").

[441] The Digital Advertising Alliance principles provide only for opt-out control. *See supra* text accompanying notes 316–17. However, they may support opt-in for sensitive information. *See* Comment of American Association of Advertising Agencies et al. 1–2 (Oct. 19, 2016), Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (supporting opt-in consent rule for sensitive information, opt-out for "[a]ll other uses of web browsing history and application use history information").

[442] On Henry Ford's own account, one day in 1909 he announced to his employees that in the future the Ford Motor Company would produce only one model of car, the Model T, and that "[a]ny customer can have a car painted any colour that he wants so long as it is black." HENRY FORD, MY LIFE AND WORK 72 (1922).

prefer a product whose acquisition or use entails a lesser exposure of one's personal information.

Across a variety of categories of goods and services that consumers may obtain using Internet-enabled data flows, there are major variations in the feature-sets of products that different vendors offer. Some search engines work better than others. Sources of news span a wide range of ideological orientations; if you want to get your news from Fox News but do not like its privacy policy, MSNBC is not a good substitute even if it has a better privacy policy.[443] If you are looking for a free game to play on your smartphone, Super Mario Run will not be a close substitute for Wheel of Fortune. Some connected home security cameras have a well-designed interface; others not so much. So, the decision to acquire a substitute product from a different vendor as a means of reaping the benefits of a more favorable privacy policy may have a high cost in terms of accepting less-desirable product features.

The expected gain from the more-favorable privacy policy, on the other hand, is likely to be small. This follows from the great uncertainty inherent in determining what impact dealing with a vendor with a particular privacy policy will have. As discussed above, privacy policies are generally vague enough, data analytics are so capable and inscrutable, and the privacy ecosystem is so complex that, in most cases, it is impossible to know whether switching vendors to get a more-favorable privacy policy will yield any tangible benefits whatsoever, let alone to come up with a reasonably accurate estimate of its magnitude.

Fifth, if people do not in fact seek out additional information about the costs and benefits of giving up their PII before deciding whether to disclose it, this is an indication that it is rational to do so. If one assumes that people generally behave rationally—and, as noted above, this is the premise of the notice-and-choice paradigm[444]—then what most of them do is some evidence of what constitutes rational behavior under the circumstances.

Personal experience, confirmed by survey evidence,[445] establishes that few people read privacy policies or change their behavior based on the content of those policies. This is some evidence that, for a rational individual, the cost of learning about the privacy practices of vendors that he is considering engaging with exceeds the expected gain. The evidence is not conclusive—it could be that consumers invest an inefficiently low amount of effort in reading privacy policies due to some misapprehension of the attendant benefits or costs. But I know of no evidence supporting that alternative interpretation.

The conclusion to which the above discussion leads is that a rational individual, deciding *ex ante* how much effort to put toward availing himself of the opportunity to promote his interests by making use of the tools that the notice-and-choice paradigm offers, would conclude that very little of such effort would be cost effective. In terms of the rubric introduced above, an individual who chooses not to read privacy policies may well be rationally inattentive. This conclusion does not imply that a rational

---

443 *See* Pamela Engel, *Here's How Liberal or Conservative Major News Sources Really Are*, BUS. INSIDER (Oct. 21, 2014), http://www.businessinsider.com/what-your-preferred-news-outlet-says-about-your-political-ideology-2014-10.

444 *See supra* text accompanying note 378.

445 *See, e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1884, 1884 n.14 (2013) (citing sources supporting the claim that "[m]ost people do not read privacy notices on a regular basis").

individual must entirely ignore the privacy policies of companies with which she is considering engaging. The idea underlying rational inattention is that investing in acquiring information relevant to a decision may be welfare-enhancing up to a certain point, but beyond that point the costs of expending additional effort to acquire more information exceed the expected benefits. So it is worth considering under what circumstances paying attention to privacy notices and choosing with whom to deal based on those notices will be cost-justified. Based on the factors discussed above, to get the most bang for his privacy-policy-reading buck, an individual should focus on gathering information where (1) she can obtain the information at relatively low cost, (2) the additional information will do a lot to reduce uncertainty about the impact of revealing her PII, (3) alternative providers offer more favorable privacy policies, and (4) the good or service is a commodity product whose features vary from one supplier to another only in the supplier's privacy practices and perhaps the price.

Thus, a rational individual might conclude that reading privacy policies is worthwhile if the relevant policies are brief and clearly written; the individual has reason to believe that there are multiple suppliers of the product, some but not all of which state that the supplier will not share the information with any third party; the supplier under consideration offers privacy choices, allowing the individual to opt-out of certain uses of his PII; the supplier is not itself in the business of combining the information the individual provides with other private information it obtains from other sources and from which it draws inferences (i.e., not Google, Facebook, Amazon, or other companies that function more like a platform than a vendor); and the product is a commodity good rather than a complex service.

2. Notice-and-Choice Cannot Work in the Context of Internet-Enabled Data Flows Because the Uniformity of Privacy Practices Leaves Little or No Room for the Exercise of Choice

As discussed above,[446] an analysis of the privacy policies of the most-visited commercial websites, most-downloaded mobile apps, and a sampling of IoT devices reveals that there is very little variation among them. Nearly all of them use both direct and surreptitious means to collect PII from users, and nearly all release that PII into the information ecosystem to be used by profit-maximizing entities, governments, criminals, and others for purposes that most of us cannot fathom.[447]

There is no reason to expect this situation to change. The obstacles to the emergence of a market structure in which providers of goods and services via Internet-enabled data flows compete for customers by battling to offer the most privacy-protective terms have proven insuperable at every phase of the development of the online information ecosystem over the past twenty years.

In the absence of viable choices among privacy terms, notice-and-choice offers only an illusion of control, not the real thing.

3. Notice of Privacy Policies Cannot Attain General Standards of Conspicuousness

As discussed above,[448] the various statements of the FIPPs, and their implementations in positive law and self-regulatory schemes, do not specify that the

446 *See supra* text accompanying notes 400–38.

447 *See supra* Tables 1 & 2.

448 *See supra* text accompanying notes 354–63.

notice must be so designed that it is likely to come to the attention of the data subject to whom it is addressed. Privacy notices accompanying websites, mobile apps, and IoT devices typically will not come to the attention of a data subject who does not actively seek them out.

This indifference to whether the message reaches the addressee is starkly at odds with basic consumer protection law. The FTC's position on how online advertising disclosures should be conveyed states a functional criterion for "clear and conspicuous" disclosures: the adequacy of a disclosure "is measured by its performance—that is, how consumers actually perceive and understand the disclosure within the context of the entire ad. . . . Simply making the disclosure available somewhere in the ad, where some consumers might find it, does not meet the clear and conspicuous standard."[449]

Privacy notices are almost never presented to the data subject front-and-center. On websites, the typical convention is to place a link on the bottom of the home page labeled "Privacy Policy" (or something less informative, like "Terms of Use" or "Legal"). Privacy policies accompanying mobile apps from the two major app platforms are accessed from a link near the bottom of the app's page.[450] IoT device privacy notices are less uniformly placed, harder to find, and mostly not available at all before purchase and installation of the device.[451] This is precisely what the FTC says advertisers may *not* do if they want to avoid being charged with false advertising: place an important disclosure in a location "where some consumers might find it" but very few actually will.[452]

Not only does this presentation of privacy policies fail to comport with consumer protection law, it also fails to meet the level of conspicuousness necessary to support a contract. In the terminology that has become standard in connection with online contracting, the typical presentation of privacy policies is analogous to "browsewrap."[453] This designates would-be contractual terms that are available somewhere on a website—often by clicking on a link at the bottom of the website's home page labeled "Terms of Use" or the like—but are not brought to the attention of the website visitor.[454] Browsewrap terms are enforceable only if the user is on notice

---

449 FTC, .COM DISCLOSURES, *supra* note 163, at 6.

450 Lisa Gutermuth, *How to Understand What Info Mobile Apps Are Collecting About You*, SLATE (Feb. 24, 2017), http://www.slate.com/articles/technology/future_tense/2017/02/how_to_understand_what_info_mobile_apps_collect_about_you.html.

451 *See supra* text accompanying paragraph preceding note 439.

452 FTC, .COM DISCLOSURES, *supra* note 163, at 6.

453 The most influential early treatment of browsewrap is in an opinion by the Second Circuit Court of Appeals. Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 32 (2d Cir. 2002) (stating that under the circumstances presented, "a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms").

454 Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1176 (9th Cir. 2014) (describing a typical browsewrap presentation, in which the purported terms are "posted on the website via a hyperlink at the bottom of the screen" and the user is not required to take any affirmative action indicating assent to the terms).

of them—either actual or constructive.[455] Courts will find that a user was on "constructive notice" of browsewrap terms only if the hyperlink leading to the terms is clearly and prominently presented.[456] A link at the bottom of a web page labeled "Privacy," in small print, with no effort made to draw the user's attention to it, does not meet that standard.[457]

The analogy to consumer protection law and contract law is instructive because those bodies of law reflect what regulators and judges have found essential to conveying information to consumers: the presentation of the information must be such that it is likely to come to the attention of a reasonable person.[458] Privacy notices, as they have been mandated by various formulations of the FIPPs, required by positive law, and implemented voluntarily, do not satisfy that criterion.

If so, why not solve the problem by simply requiring privacy notices to be posted "clearly and conspicuously," as advertising disclosures and contract terms must be if they are to have legal validity? A moment's reflection will make evident the infeasibility of such a rule.

First, this proliferation of notices would severely detract from the user experience. Each time a user visited a website, accessed a mobile app, or set up an IoT device, she would be presented with a privacy notice in a manner intrusive enough to qualify as conspicuous. If the information being conveyed is complex, as is the case with privacy policies, the FTC is willing to accept placement of the material such that the site visitor must click on a hyperlink to view it.[459] The adequacy of such an approach will depend on "the placement and prominence of the hyperlink on the webpage or screen" as well as how the hyperlink is labeled.[460] This likely means that the link would have to squarely confront the user from a location on the home page of the website—perhaps via a banner that is plastered across the screen.[461] Because users frequently access

---

[455] Nicosia v. Amazon.com, Inc., 834 F.3d 220, 233 (2d Cir. 2016) ("In determining the validity of browsewrap agreements, courts often consider whether a website user has actual or constructive notice of the conditions.").

[456] *Id.* ("Clarity and conspicuousness of . . . terms are important in securing informed assent." (quoting *Specht*, 306 F.3d at 30)); *id.* ("[W]hen terms are linked in obscure sections of a webpage that users are unlikely to see, courts will refuse to find constructive notice.").

[457] *See, e.g.*, *Nguyen*, 763 F.3d at 1178–79 (no assent "where a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent"); Roller v. TV Guide Online Holdings, LLC, 2013 Ark. 285, 285 (2013) (no assent to terms "accessible via hyperlink at the bottom of each page of the website"); Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362, 367 (E.D.N.Y. 2009) (no assent where user "could not even see the link to [the terms] without scrolling down to the bottom of the screen"), *aff'd*, 380 F. App'x 22 (2d Cir. 2010).

[458] *See supra* notes 449, 453–57 and accompanying text.

[459] FTC, .COM DISCLOSURES, *supra* note 163, at 10.

[460] *Id.* at 10–11.

[461] This is how certain privacy disclosures are typically made on websites within the jurisdiction of European Union law. A 2009 directive requires website operators to obtain a site visitor's consent before placing a cookie on her computer. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, art. 2(5), 2009 O.J. (L 337) 11, 30. Many website operators in the EU have complied with this rule by slapping a banner along the top or bottom of the website's home page, with wording something like: "This website uses

websites via a link from another website that takes them to an interior page rather than the home page, the disclosure link would have to appear conspicuously on each page of a website through which collection of a user's information occurs. For a website that a user views on the monitor of a laptop or desktop computer, this could be done with some sacrifice to the design integrity of the site and the user experience. However, for websites and mobile apps that a user views on a smartphone screen, the sacrifice would be more severe, as a larger proportion of the home screen would be taken up by the hyperlink.[462]

Second, if all websites, mobile apps, and IoT devices *did* implement clear and conspicuous notice of the relevant privacy policies, the result would be staggeringly useless. The proliferation of notices would soon fade into the background and be completely ignored, a victim of the cognitive limitations that are a feature of humanity. Notice everywhere is no notice at all. Beyond that, the nonstop, in-your-face notices of the availability of privacy policies would likely not bring about a single additional reading of a privacy policy. We ignore privacy policies because we are unable to perceive any benefit in doing so; easier access to the notices would not change that calculus.

Clear and conspicuous disclosure in advertisements and contracts works because we engage with relatively few of them. We do not make purchases at anywhere near the rate at which we click from one website to another or tap to open another mobile app. When making a purchase involving a meaningful amount of money, we have incentive to expend the effort needed to read and understand the advertising claims and disclosures as well as the contract terms. The same system could not feasibly be applied to all websites, mobile apps, and IoT devices that collect personal information.

#### 4. Notice-and-Choice Amounts to Blanket Consent Due to the Non-Transactional Nature of Privacy Interactions

The notice-and-choice procedure was designed for a transactional scenario that is presently the exception rather than the rule in consumers' interactions with websites, mobile apps, and IoT devices. In the prototypical scenario, the data collector offers a transaction and among the proposed terms is the privacy policy. The data subject accepts the terms by engaging in the transaction, exercising her choice to allow use of her PII as specified in the notice. Conceptually, the privacy policy is assimilated to a contract term.

But most data collection situations using the facilities of Internet-enabled data flows involve an ongoing relationship between the parties, with consent sought only at the outset of the relationship. A website does not inquire in advance of each collection of clickstream data whether the user consents to that collection, and neither does a mobile app. An IoT device may collect personal information continuously for years at a stretch.

---

cookies. By using this website and its offers and continuing navigating, you accept these cookies. You can change them in your browser settings." *See, e.g.*, AUDI, http://www.audi.com/en.html (last visited Jan. 21, 2018). Anybody who has viewed more than a few of these websites has learned to ignore the cookies notification.

462 The FTC emphasizes that the disclosure method must be one that remains conspicuous regardless of "the various programs and devices" that might be used to access the material. FTC, .COM DISCLOSURES, *supra* note 163, at 12.

Because of the ongoing nature of our engagement with websites, mobile apps, and IoT devices, the consent a user provides through the notice-and-choice procedure amounts to blanket consent: consent to whatever data collection and use the collector decides to engage in, now and into the indefinite future, without a specification of each such collection and use. Because the consequences of granting blanket consent to use one's PII cannot be known at the time the consent is granted, this mechanism does not allow an individual to exercise meaningful control over disposition of his PII.

In other privacy-related contexts, blanket consent is disfavored, such as consent to research uses of one's DNA,[463] general consent to medical procedures that is interpreted as including consent to drug testing,[464] and consent to disclosure of communications with one's therapist.[465] Blanket consent is contrary to the EU Data Protection Directive.[466]

The Video Privacy Protection Act of 1998 generally prohibits a video tape provider from disclosing its customers' viewing habits absent the customer's consent.[467] As originally enacted, the statute banned blanket consent, requiring "the informed, written consent of the consumer given *at the time the disclosure is sought*."[468] In 2013, Congress amended the statute to allow a form of blanket consent but limited that consent to a two-year period; consent may now be "given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner."[469] The original prohibition of blanket consent to disclosure of private information, together with the two-year limitation in the amended provision, indicates the controversial status of blanket consent in privacy contexts.

---

[463] Julie A. Burger, *What Is Owed Participants in Biotechnology Research?*, 84 CHI.-KENT L. REV. 55, 61 (2009) (quoting COMMITTEE ON HUMAN GENOME DIVERSITY, NAT'L RES. COUNCIL, EVALUATING HUMAN GENETIC DIVERSITY 65 (1997)) ("'It is not ethically or legally acceptable to ask research participants to "consent" to future but yet-unknown uses of their identifiable DNA samples.'").

[464] Derk B.K. VanRaalte IV, *Punitive Policies: Constitutional Hazards of Non-Consensual Testing of Women for Prenatal Drug Use*, 5 HEALTH MATRIX 443, 469–70 (1995) (arguing that a pregnant woman's signing of a blanket consent upon admission to a hospital is inadequate to justify testing her for illegal drugs).

[465] Illinois Mental Health and Developmental Disabilities Confidentiality Act, 740 ILL. COMP. STAT. 110/5(c) (2018) (indicating that a patient's blanket consent to disclosure of her communications with a mental health therapist is invalid).

[466] The Directive's definition of "consent" requires "specific" consent. Data Protection Directive, *supra* note 151, art. 2(h). The Article 29 Working Party interprets this as forbidding blanket consent: "To be valid, consent must be specific. In other words, blanket consent without specifying the exact purpose of the processing is not acceptable." Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent, 01197/11/EN, WP187 (July 13, 2011), at 17.

[467] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(1) (2018).

[468] Video Privacy Protection Act of 1988, Pub. L. No. 100-618, § 2(b)(2)(B), 102 Stat. 3195 (1988) (emphasis added).

[469] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(2)(B)(ii)(II) (2018). Netflix lobbied for passage of the amendment so that it could share its customers' viewing selections on Facebook. Kathryn Elizabeth McCabe, *Just You and Me and Netflix Makes Three: Implications for Allowing "Frictionless Sharing" of Personally Identifiable Information Under the Video Privacy Protection Act*, 20 J. INTELL. PROP. L. 413, 416 (2013).

Karl Llewellyn famously proposed "blanket assent" as a conceptual solution to the dilemma inherent in standard-form contracting, where the purchaser has no opportunity to bargain over the terms (other than, perhaps, the price) and yet is held bound to them.[470] His idea was that when an individual enters into a transaction, she accepts all of the non-negotiable terms to the extent they are "not unreasonable or indecent" or not "manifestly unreasonable and unfair."[471] But blanket assent has no justification in a situation where nobody, neither the data subject who is deemed to assent to collection and use of his PII nor the collector itself, can say *ex ante* what uses will be made of the information and what impact those uses will have on the data subject.

Because consent to the privacy terms adopted and disclosed by websites, mobile apps, and IoT devices amounts to blanket consent, it cannot be regarded as effective consent. Notice-and-choice cannot be justified as a fair information practice principle in these contexts.

5. Notice-and-Choice Cannot Work When PII Is Transferred to a Third Party for Uses that Are Not Disclosed and Could Not Be Disclosed Because Not Known to the Transferor

The private-data ecosystem deviates from the transactional model in another way as well. When a person uses a website, mobile app, or IoT device, she is dealing not just with the operator of the website, the supplier of the mobile app, or the manufacturer of the IoT device. Third parties are lurking in the shadows, in the form of advertising networks that acquire clickstream information in real time and data brokers that combine private with public information and perform analytics yielding conclusions that have economic value.

The individuals involved do not receive adequate notice of the uses that these third parties make of their private information. Few consumers are aware of the activities, or even the existence, of these third parties.[472] Website privacy policies commonly disclose that the site visitor's private information may be supplied to third parties.[473] But that sort of notice is not of much use to the individual because it does not disclose what uses the third party will make of the information.

Even if a website operator wanted to provide site visitors with full disclosure about the downstream uses of the information it collects from them, it could not. The website operator will generally have no more idea of what happens to the data once it is passed along to a third party than does the data subject himself. Both the vastness of the task, and the impossibility of specifying what uses third parties may find for the data at

[470] KARL N. LLEWELLYN, THE COMMON LAW TRADITION: DECIDING APPEALS 370 (1960).

[471] *Id.* at 371.

[472] Regarding data brokers, the FTC observes: "Because these companies generally never interact with consumers, consumers are often unaware of their existence, much less the variety of practices in which they engage." FTC, DATA BROKERS, *supra* note 29, at i. The data brokers that the FTC studied are Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future—not exactly household names. *Id.* at 8–9. The same can be said of advertising networks. The Digital Advertising Alliance's opt-out list currently includes 133 companies, the alphabetically ordered list beginning with 12 Digit Marketing, 33Across, Accuen, ActionX, AcuityAds, etc. The full list may be viewed by following the DAA's opt-out procedure, starting from http://optout.aboutads.info.

[473] *See supra* Table 1.

some future date, would doom to failure any effort to assemble information about these uses and present it to a user in an actionable form.

The notice-and-choice model was not designed for, and simply cannot effectively deal with, the complexities of a data ecosystem that inscrutable third parties dominate.

#### 6. Notice-and-Choice Cannot Work with Some Types of IoT Devices Because Third Parties Cannot Consent

Some IoT devices collect personal information about data subjects whose only connection to the device is being in range of it. Home surveillance cameras capture the activities of visitors. Artificially intelligent interactive toys, like Hello Barbie, can capture the speech of the owner's playmates.[474] Video doorbells capture images of a person approaching the front door. Regardless of whether the owner of the device has consented to the collection and use of his own information, he cannot consent on behalf of third parties, and seeking consent directly from those parties would be highly impractical.

## V. MOVING TO A NEW PARADIGM

If notice-and-choice cannot meet the goals of the fair information practice principles when applied to websites, mobile apps, and IoT devices, what is the alternative? I propose that the purely procedural approach of notice-and-choice should be supplemented by one that takes into account the substance of a data collector's privacy rules.

### *A. Substantive Rules of Privacy in Legislation Are Not a Novelty*

The dominant role that the FIPPs have come to play in our thinking about information privacy, founded as they are on the proceduralist paradigm of notice-and-choice, tends to obscure the fact that substantive rules protecting privacy are not only thinkable but are actually in use. While most privacy laws are strictly procedural, allowing data collectors to do whatever they want with personal information as long as (in some cases) they notify the data subject of those uses, some privacy laws do include substantive limitations. For example:

- The FTC's regulation under COPPA prohibits the operator of a website "from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity."[475]
- The Telecommunications Act of 1996 provides that a telecommunications carrier may not use metadata it received from another carrier to engage in marketing.[476]
- The Fair Credit Reporting Act provides that a consumer credit reporting agency may not include in a credit report the identity of a

[474] Walker, *supra* note 98.

[475] 16 C.F.R. § 312.7 (2018).

[476] Telecommunications Act of 1996, 47 U.S.C. § 222(b) (2018).

furnisher of medical information if doing so would identify the provider of the medical service or its nature.[477]

- The FCC's (invalidated) ISP privacy rules prohibit broadband Internet access service providers "from conditioning the provision of broadband service on a customer surrendering his or her privacy rights" and "from terminating service or otherwise refusing to provide [Internet access] due to a customer's refusal to waive any such privacy rights."[478]
- European Union law restricts a data processor from processing designated categories of sensitive data.[479]

In addition, several prominent policy discussions of fair information practice principles have advocated the deployment of certain substantive limitations on users of private information. During the discussions of the committee that produced the 1973 HEW Report, several speakers thought that part of the solution was the establishment of substantive privacy rules.[480] The 1995 IITF policy paper called for the institution of basic privacy protections in certain situations.[481] In its 2012 report, the FTC proposed a substantive limitation on a business's privacy practices: no matter what procedures it follows, a company offering an important product or service without many good substitutes may not engage in privacy-invading uses of a customer's data that are not germane to the transaction.[482] Recent examinations of the

---

[477] Fair Credit Reporting Act, 15 U.S.C. § 1681c(a)(6) (2018).

[478] FCC, ISP Privacy Rules, *supra* note 294, ¶ 295.

[479] The EU Data Protection Directive allows member states to forbid the processing of sensitive data, even with the data subject's consent. The general rule is: "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." Data Protection Directive, *supra* note 151, art. 8(1). There is an exception if the data subject gives "explicit consent," but a member state may void that exception making the prohibition non-waivable. *Id*. art. 8(2)(a). The EU's new privacy regulation has a similar rule, extending the categories of sensitive data to include genetic and biometric data. GDPR, *supra* note 151, art. 9(1), 9(2)(a).

[480] Transcript of Proceedings, Secretary's Advisory Committee on Automated Personal Data Systems 43 (May 19, 1972) ("I think we have to go beyond that and draw the line, difficult as it may be, of the right of the employer to collect personal information and the right of the employee to be free from undue invasion of his privacy.") (Kenneth A. McLean); Transcript of Proceedings, Secretary's Advisory Committee on Automated Personal Data Systems 44–45 (Sept. 30, 1972) ("The idea is to create or to recommend that legislation be instituted that would define penalties for unreasonable use of information. . . . The idea would be to create legislation which would include both criminal and civil penalties and probably one would be wise to make it a class actionable offense, if institutions were to do certain things that we would define as unreasonable use of information.") (Willis H. Ware).

[481] "[I]n certain cases—for example, if the individual lacks sufficient bargaining power—purely contractual arrangements between individuals and information users may fail to respect privacy adequately. In such instances, society should ensure privacy at some basic level in order to satisfy the Information Privacy Principle." NAT'L INFO. INFRASTRUCTURE TASK FORCE, *supra* note 193, ¶ 4.

[482] FTC, PROTECTING CONSUMER PRIVACY, *supra* note 7, at 52 (noting that where there are few alternative suppliers of Internet access, "the service provider should not condition the

consequences of widespread processing of "big data" have suggested that privacy rules should aim at controlling the practices of data *users*, rather than being limited to the context of data *collection*.[483]

Thus, precedent exists for legislative bodies to prescribe substantive rules protecting privacy based on public policy considerations.

### *B. The General Doctrines of Unfairness and Unconscionability Can Support Substantive Privacy Rules*

The common law developed doctrines, later codified, that allow courts and law enforcement agencies to nullify practices that are inimical to consumer interests. These doctrines—unfairness and unconscionability—have been deployed against invasions of privacy and failure to maintain reasonable data security practices. They could be used, either in case-specific situations or as the conceptual underpinnings of legislative rules, to generate substantive privacy standards applicable to Internet-enabled data flows.

#### 1. Unfairness

Contrary to the everyday usage of the term, a determination that conduct is "unfair" is not merely a moral judgment but rather a legal conclusion. The doctrine evolved through common law methods and was later codified. Beginning in the mid-19th century, the courts developed a federal common law of trade regulation.[484] Rules prohibiting unfair competition were first applied in situations involving passing off one's goods as those of another and misappropriation.[485] This was the background against which Congress enacted the FTC Act.

As originally enacted in 1914, the Act forbade "unfair methods of competition in commerce."[486] From the start, the FTC applied this language to both deceptive advertising and misuse of concentrations of commercial power, considering both to be "unfair" and to interfere with competition.[487] In 1922, early in the life of the FTC Act, Sears, Roebuck & Company sought to avoid a determination that its advertisements were false and therefore amounted to "unfair methods of competition" on the ground that the term was too indefinite to have any application beyond acts that the common law had found unfair as of the 1914 enactment of the Act. The court held that the term, even then, had a reasonably ascertainable meaning: the FTC commissioners "are to exercise their common sense, as informed by their knowledge of the general idea of

---

provision of broadband on the customer's agreeing to, for example, allow the service provider to track all of the customer's online activity for marketing purposes").

[483] *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 59, at 56; PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 380, at xii; Craig Mundie, *Privacy Pragmatism: Focus on Data Use, Not Data Collection*, FOREIGN AFF., Mar.–Apr. 2014, at 28, 29.

[484] Peter S. Menell, *Regulating "Spyware": The Limitations of State "Laboratories" and the Case for Federal Preemption of State Unfair Competition Laws*, 20 BERKELEY TECH. L.J. 1363, 1381 (2005).

[485] *Id.* at 1382. Unfair competition law was later codified as federal trademark law, the current instantiation of which is the Lanham Act, 15 U.S.C. §§ 1051–1141 (2018).

[486] Federal Trade Commission Act of 1914, Pub. L. No. 63-203, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § 45(a)).

[487] HOOFNAGLE, *supra* note 378, at 3–4.

unfair trade at common law, and stop all those trade practices that have a capacity or a tendency to injure competitors directly or through deception of purchasers."[488]

In 1938, Congress amended the FTC Act by granting the Commission the authority to prevent "unfair or deceptive acts or practices" in addition to "[u]nfair methods of competition."[489] The purpose of the amendment was to broaden the FTC's authority to control deceptive advertising by eliminating any need to prove harm to competitors.[490] When exercising its statutory authority to prevent unfairness in consumer protection contexts, the FTC relies upon the "unfair . . . acts or practices" language of this amendment.[491]

In 1994, adopting the FTC's own formulation of what makes an act or practice "unfair," Congress codified the criterion in these terms:

> The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[492]

Thus, an "unfair" practice is one that (1) "causes or is likely to cause substantial injury to consumers" (2) "which is not reasonably avoidable by consumers themselves" and (3) "not outweighed by countervailing benefits to consumers or to competition."[493] The determination may be informed by, but not based exclusively on, "public policy considerations" untethered from the statutory text.[494]

All of the states have laws, often called Unfair and Deceptive Acts and Practices ("UDAP") laws or "Little FTC" acts, prohibiting "unfair" practices.[495] Some but not

---

[488] Sears, Roebuck & Co. v. FTC, 258 F. 307, 311 (7th Cir. 1919).

[489] Wheeler-Lea Act of 1938, Pub. L. No. 75-447, ch. 49, § 3, 52 Stat. 111 (1938) (current version at 15 U.S.C. § 45 (2018)).

[490] HOOFNAGLE, *supra* note 378, at 37; Menell, *supra* note 484, at 1383.

[491] *See, e.g.*, Complaint ¶ 17, *In re* Aaron's, *supra* note 92.

[492] Federal Trade Commission Amendments Act of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (1994) (codified at 15 U.S.C. § 45(n)). The amendment partially codified the FTC's 1980 Policy Statement on Unfairness (appended to *In re* International Harvester Co., 104 F.T.C. 949, 1070 (1984)).

[493] 15 U.S.C. § 45(n) (2018).

[494] For a history and evaluation of the FTC's unfairness authority, see J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FED. TRADE COMM'N (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

[495] CAROLYN L. CARTER, NAT'L CONSUMER LAW CTR. INC., CONSUMER PROTECTION IN THE STATES (2009), www.nclc.org/images/pdf/udap/report_50_states.pdf. These laws vary substantially in the scope and strength of their protections. *Id.* at 7–10.

all of these state laws are interpreted according to the FTC's unfairness standard.[496] Thus, an expansive body of law evaluates commercial practices to determine whether they should be banned as "unfair."

*a. "Unfairness" Applied in Privacy Contexts*

Precedent supports invoking statutory prohibitions of unfair commercial practices to counter invasions of privacy. In recent years,[497] the FTC and state agencies have applied their unfairness authority in a number of situations involving information privacy or the related subject of information security.[498]

In *FTC v. VIZIO, Inc.*,[499] the FTC and the New Jersey Attorney General brought an action against a manufacturer of Internet-connected television sets that, according to the complaint, "continuously track what consumers are watching, and transmit that information" back to VIZIO "on a second-by-second basis."[500] VIZIO provided the information to third parties, which used it among other things "for the purpose of targeting advertising to particular consumers on their other digital devices based on their television viewing data."[501] VIZIO did not adequately disclose these practices to purchasers of the televisions.[502] The complaint charged that this undisclosed collection and dissemination of personal data was unfair, reciting the three statutory elements of an unfairness claim.[503] Settling the case, the parties agreed to a stipulated order that prohibits the collection of viewing data unless VIZIO provides notice and obtains the consumer's consent.[504]

---

[496] Most of the state "unfairness" laws are interpreted according to a standard that the FTC devised in 1964 but has since discarded. *See* JONATHAN SHELDON & CAROLYN L. CARTER, NAT'L CONSUMER LAW CTR. INC., UNFAIR AND DECEPTIVE ACTS AND PRACTICES 197 (6th ed. 2004) (discussing the "*S&H*" standard).

[497] In its earlier cases dealing with online privacy, and in most of the more recent ones too, the FTC charged the respondent with deception rather than unfairness. The first such case was *In re* Geocities, No. C–3850 (F.T.C. Feb. 5, 1999). Other cases in this vein include: *In re* Goldenshores Technologies, LLC, No. C–4446 (F.T.C. Mar. 31, 2014) (flashlight app's privacy policy says that app will collect information related to app's functioning; failure to disclose that it also collects user's location information and transmits it to advertisers alleged to be deceptive); *In re* Facebook, Inc., No. C–4365 (F.T.C. July 27, 2012) (deceptive statements about privacy settings); and *In re* Google Inc., No. C–4336 (F.T.C. Oct. 13, 2011) (deceptive statements involving Google Buzz). A company's privacy practices may be charged as deceptive only if the company has made some representation that is false. The cases discussed in this Section involved privacy-harming conduct that did not include any such representations and thus could only be charged as unfair.

[498] Both information privacy and information security are concerned with disclosures of personal information. They differ in that the latter involves unauthorized access to the information through inadequate security measures.

[499] FTC. v. VIZIO, Inc., No. 2:17-CV-00758 (D.N.J. Feb. 6, 2017).

[500] Complaint ¶¶ 12–14, *id.*

[501] *Id.* ¶ 16(c).

[502] *Id.* ¶¶ 19–22.

[503] *Id.* ¶¶ 32–34.

[504] Stipulated Order for Permanent Injunction and Monetary Judgment at 4–5, FTC v. VIZIO, Inc., No. 2:17-CV-00758 (D.N.J. Feb. 6, 2017). The order specifies that the notice must

In *In re Aaron's, Inc.*,[505] the FTC charged Aaron's, which operated a chain of stores that rent household items to consumers, with unfairness in connection with its installation and use of monitoring and geotracking software on the computers it rented. According to the complaint, some of Aaron's franchisees installed software called PC Rental Agent on these computers.[506] The software allowed Aaron's employees to "surreptitiously monitor the activities of computer users, including by logging keystrokes, capturing screenshots, and using the computer's webcam." It also allowed them to track the physical location of the computers.[507] Needless to say, this allowed Aaron's to collect highly sensitive information as well as "photographs of computer users and anyone else within view of the camera."[508] This occurred "[i]n numerous instances" without notice to or consent from the consumers.[509] The complaint alleged that this privacy-invading conduct by Aaron's was unfair and violated the FTC Act.[510]

The consent order settling the action contained injunctive provisions that treat the collection of information separately from the geotracking.[511] The order prohibited "[u]sing any monitoring technology to gather data or information from or about a consumer from any computer rented to a consumer" except, with the consumer's consent, to provide technical assistance to the consumer.[512] That is, the order flatly prohibits Aaron's use of monitoring technology to promote its own interests, even with the consumer's consent. Geotracking is forbidden unless Aaron's first provides "clear and prominent notice" to the consumer and obtains his "affirmative express consent."[513]

---

be "prominent[]" and "separate and apart from any 'privacy policy,' 'terms of use' page, or other similar document." *Id.* at 4. Consent must be opt-in, requiring "affirmative express consent." *Id.*

505 *In re* Aaron's, Inc., No. C–4442 (F.T.C. Mar. 10, 2014).

506 Complaint ¶ 4, *id.*

507 *Id.*

508 *Id.* ¶ 5.

509 *Id.*

510 *Id.* ¶¶ 16–17.

511 Decision and Order at 4–6, *id.*

512 *Id.* at 4.

513 *Id.* at 4–5. The FTC also sued DesignerWare, the maker of the PC Rental Agent Software, and Aspen Way Enterprises, one of the Aaron's franchisees that used the software. The injunctive provisions of the consent orders in those cases mirror those in the Aaron's case. *See* Decision and Order, *In re* DesignerWare, LLC, No. C–4390 (F.T.C. Apr. 11, 2013); Decision and Order, *In re* Aspen Way Enters., Inc., No. C–4392 (F.T.C. Apr. 11, 2013).

Other cases in which the FTC charged a privacy-harming practice as unfair include: FTC v. Blue Global, LLC, No. 2:17-cv-02117-ESW (D. Ariz. July 3, 2017) (defendant negligently transmitted consumers' sensitive financial information, which they submitted seeking loans, to third parties who were not lenders); *In re* Brittain, No. C–4564 (F.T.C. Dec. 28, 2015) (posting nude photographs on a revenge-porn site; order bans posting without consent); FTC v. Sitesearch Corp., No. CV-14-02750-PHX-NVW (D. Ariz. Dec. 11, 2015) (defendant collected sensitive financial information from consumers seeking payday loans and deliberately sold the loan applications to non-lenders; order prohibits transferring sensitive information without consent); *In re* Facebook, Inc., No. C–4365 (F.T.C. July 27, 2012) (making postings that users

In these two cases, the injunctive relief takes two different forms. One form prohibits privacy-invasive conduct, *unless* accompanied by robust notice-and-consent,[514] while the other form flatly prohibits the conduct.[515] The former remedy implies that the violation consisted of acquiring a person's private information without first notifying him of the collection and obtaining his consent—a violation of a *procedural* rule. The latter is premised on a different sort of violation: collecting the information at all. This is a violation of a *substantive* rule. The former remedy's premise is that notice-and-choice is capable of performing its function as one of the fair information practice principles, as long as it is implemented correctly. The latter recognizes that all the notice and choice in the world will not solve the problem.

*VIZIO* and *Aaron's* are particularly inappropriate cases for the procedural remedy that the FTC applied to some of the claims. Both cases involved the purchase (or rental) of physical objects, rather than, say, access to a website or mobile app. Put yourself in the place of the purchaser of a VIZIO sixty-five-inch-diagonal television set. This is a large and heavy item. You might have struggled to get it into the back of your car from the curbside of a Best Buy store or borrowed a friend's truck for the purpose because your car was too small. Or you might have bought the television online from Overstock.com and received it in a delivery from UPS or FedEx. After spending a fair amount of time extracting it from the box, assembling it, setting it up, and getting it to work with your home network, the television presents you with a prominent notice, requesting your consent to allow VIZIO to continuously track what you watch, "on a second-by-second basis,"[516] and to transmit that information to third parties who will use it to target advertising through your other connected devices.

At this point, do you have a meaningful opportunity to exercise choice about whether to share your personal information? If you click "I Disagree," the television set will politely inform you that you cannot use it and you should return the set to the vendor.[517] That will require you to fit the various components back into the box, seal it up, and haul it back to the Best Buy or obtain a return authorization from Overstock.com so the delivery service can pick it up. You may not get all of your

had designated as restricted publicly available; order prohibits doing so without the poster's consent); *In re* Vision I Properties, LLC, No. C–4135 (F.T.C. Apr. 19, 2005) (online shopping cart provider sold consumer information to third parties; remedy allows continuation of conduct if notice is supplied).

514 As in the *VIZIO* case, Stipulated Order for Permanent Injunction and Monetary Judgment at 17–18, *VIZIO*, *supra* note 504, and the geotracking claim in *Aaron's*, Decision and Order at 4–5, *In re* Aaron's, Inc., No. C–4442 (F.T.C. Mar. 10, 2014).

515 As in the monitoring claim in *Aaron's*. Decision and Order at 4, *In re* Aaron's, *supra* note 514.

516 *See supra* text accompanying note 500.

517 Actually, it might not. VIZIO's current privacy policy says that you can turn off the information-collection in the television set's settings. *How to Turn On or Off Video ACR/Viewing Data Collection (Also Known as "Smart Interactivity")*, VIZIO, https://www.vizio.com/viewingdata (last visited Aug. 8, 2017). However, the FTC's order does not require the company to allow the user to keep the television while disabling the privacy-invasive functions. The point holds generally for IoT devices.

money back; Best Buy charges a restocking fee on certain items,[518] and if you return a box that has been opened, Overstock.com will only refund seventy percent of the purchase price.[519] You will probably also have to pay the return shipping fee.

Faced with all of this hassle and expense, will you still click "I Disagree"? Or will you recognize ruefully that resistance is futile: you cannot know whether the harms you will suffer from VIZIO's collection of your viewing information and transmission of it to unidentified third parties will exceed the costs of returning the television. Besides, all other manufacturers of connected televisions probably are engaging in the same privacy-invading conduct to maximize their revenues, so your only options are to give up your data or do without a smart TV.

*b. "Unfairness" Applied in Security Breach Contexts*

The FTC has also used its unfairness authority against companies whose security mechanisms and procedures, according to the agency, did not meet a reasonableness standard. The most salient of these cases is the FTC's action against LabMD, a rare FTC case in which the defendant charged with a consumer protection violation chose to litigate rather than agree to the entry of a consent order. LabMD was a medical laboratory that performed tests on tissue samples and reported the results to the referring physicians. In the course of its activities, LabMD collected sensitive personal information on over 750,000 patients. In 2005, a LabMD employee installed LimeWire, a peer-to-peer file-sharing program, on her office computer, using it to download music from the Internet. In 2008, a forensic analyst working for a data security company named Tiversa Holding Co. used LimeWire to access and download from the employee's computer a file that contained 1,718 pages of sensitive information—including names, dates of birth, social security numbers, and information about medical tests performed—belonging to 9,300 consumers. Tiversa notified LabMD of the exposure of this file (referred to in the litigation as the "1718 file") on its system and offered to sell LabMD its breach detection services. When LabMD declined to retain its services, Tiversa informed the FTC about the exposure of the file.[520]

In 2013, the FTC filed an administrative complaint against LabMD, alleging that the company "failed to provide 'reasonable and appropriate' security for personal information maintained on LabMD's computer networks, and that this conduct 'caused or is likely to cause' substantial consumer injury."[521] The complaint charged that this conduct was an unfair practice in violation of the FTC Act. After trial, the administrative law judge ("ALJ") ruled in LabMD's favor, finding that the FTC had failed to establish that LabMD's actions caused or were likely to cause "substantial

[518] *Returns & Exchanges*, BESTBUY.COM (Feb. 14, 2018), http://www.bestbuy.com/site/help-topics/return-exchange-policy/pcmcat260800050014.c?id=pcmcat260800050014.

[519] *VIZIO M55-c2 55" 4k Ultra HD Smart TV LED LCD 120Hz 3840x2160 HDTV*, OVERSTOCK, https://www.overstock.com/Electronics/VIZIO-M55-C2-55-4K-Ultra-HD-SMART-TV-LED-LCD-120Hz-3840x2160-HDTV/15814274/product.html (last visited Mar. 12, 2018) ("We will issue a partial refund of up to 70 percent if returned items have been opened, used, or returned late.").

[520] LabMD Inc. v. FTC, 678 F. App'x 816, 818 (11th Cir. 2016).

[521] *In re* LabMD, Inc., No. 9357, 2015 WL 7575033, at *2 (F.T.C. Nov. 13, 2015).

injury" to consumers, one of the elements of an unfairness claim.[522] Complaint counsel appealed the decision to the Commission, which reversed the ALJ, holding that the disclosure of the 1718 file caused substantial harm and the other elements of an unfairness violation were also satisfied.[523]

LabMD appealed the FTC's decision to the Eleventh Circuit. In 2016, the court granted LabMD's motion for a stay of the FTC's order pending appeal, having determined that "a serious legal question" existed about the correctness of the FTC's determination that the exposure of the 1718 file caused, or was likely to cause, substantial injury to consumers.[524] The court reasoned that (1) it was not clear that the statute's "substantial injury" element could be met by subjective harms like emotional impact,[525] and (2) the FTC's interpretation of the statute's "likely to cause" criterion to include "something that has a low likelihood" of occurrence is doubtful.[526]

Pending the Eleventh Circuit's decision on the merits in *LabMD*, the only litigated case testing the FTC's application of its unfairness authority in a security breach situation is *FTC v. Wyndham Worldwide Corp*.[527] In that case, inadequate security of data collected from hotel guests resulted in hackers getting access to the payment card information of over 619,000 guests through three separate attacks from 2008 to 2009, leading to over $10 million in fraudulent charges.[528] Wyndham challenged the FTC's application of its unfairness authority in this situation on several grounds, but the Third Circuit sided with the FTC. Among other things, the court rejected Wyndham's argument that application of the unfairness criterion violated its right to due process because "the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow."[529] To the contrary, the court held that the FTC's published guidance on cybersecurity, and its numerous complaints against other companies for cybersecurity failures, gave sufficient notice of what the FTC would consider unreasonable security.[530]

The FTC has invoked its unfairness authority in numerous other cases involving inadequate security of personal data, resolving them through consent decrees.[531]

---

[522] *Id*. at *9. The ALJ noted that no evidence indicated the 1718 file was downloaded by anyone other than Tiversa and that Tiversa provided it only to the FTC and an expert who had a working relationship with Tiversa. *Id.* at *46. Under these circumstances, the ALJ concluded, there could be no likelihood of harm to consumers whose private information appeared in the document. *Id.* at *46–53.

[523] *In re* LabMD, Inc., No. 9357, 2016 WL 4128215, at *14–24 (F.T.C. July 28, 2016). In the FTC's view, the release of a person's sensitive medical information is inherently injurious, even "in the absence of proven economic or physical harm." *Id.* at *14.

[524] *LabMD*, 678 F. App'x at 821.

[525] *Id.* at 820.

[526] *Id.* at 821.

[527] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

[528] *Id.* at 241–42.

[529] *Id.* at 249.

[530] *Id.* at 256–58.

[531] *See* FTC v. D-Link Sys., No. 3:17-CV-00039, 2017 WL 4150873 (N.D. Cal. Sept. 19, 2017) (failure to secure routers and IP cameras); FTC v. Ruby Corp., No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016) (inadequate security of data collected by dating website); *In re* AsusTeK

Courts have also applied state UDAP law to find privacy-invasive practices actionable as unfair.[532]

---

Computer, Inc., No. C–4587 (F.T.C. July 18, 2016) (failure to secure routers); FTC v. Bayview Solutions, LLC, No. 1:14-cv-01830-RC (D.D.C. Apr. 20, 2015) (operator and users of website that facilitated transactions between buyers and sellers of debt posted personal information without any access controls); FTC v. Cornerstone & Co., LLC, No. 1:14-cv-01479-RC (D.D.C. Apr. 20, 2015) (same); *In re* GMR Transcription Servs., Inc., No. C-4482 (F.T.C. Aug. 14, 2014) (inadequate security of personal information in transcriptions of audio files); *In re* GeneLink, Inc., Nos. C–4456, 4457 (F.T.C. May 8, 2014) (company maintained private information in a way that allowed access by affiliates); *In re* Accretive Health, Inc., No. C–4432 (F.T.C. Feb. 5, 2014) (laptop containing medical information was left in a car and stolen); *In re* TRENDnet, Inc., No. C–4426 (F.T.C. Jan. 16, 2014) (inadequate security for IP cameras); *In re* HTC America, Inc., No. C–4406 (F.T.C. June 25, 2013) (security vulnerabilities introduced into customized version of Android for mobile phones); *In re* Compete, Inc., No. C–4384 (F.T.C. Feb. 20, 2013) (failure to protect information acquired from consumers using a browser toolbar); *In re* EPN, Inc., No. C–4370 (F.T.C. Oct. 3, 2012) (debt collector's employee installed P2P filesharing software on her computer, resulting in security breach); *In re* Upromise, Inc., No. C–4351 (F.T.C. Mar. 27, 2012) (failure to protect information acquired from consumers using a browser toolbar); *In re* SettlementOne Credit Corp., No. C–4330 (F.T.C. Aug. 17, 2011) (inadequate security on consumer reports resulting in breach); *In re* ACRAnet, Inc., No. C–4331 (F.T.C. Aug. 17, 2011) (same); *In re* Fajilan and Assocs., Inc., No. C–4332 (F.T.C. Aug. 17, 2011) (same); *In re* Lookout Servs., Inc., No. C–4326 (F.T.C. June 15, 2011) (inadequate security on database of personal information resulting in breach); *In re* Ceridian Corp., No. C-4325 (F.T.C. June 8, 2011) (inadequate security on database of personal information resulting in breach); *In re* Rite Aid Corp., No. C–4308 (F.T.C. Nov. 12, 2010) (disposing of documents containing sensitive medical information in unsecured dumpsters); *In re* Dave & Buster's, Inc., No. C–4291 (F.T.C. May 20, 2010) (inadequate security of credit card information collected from restaurant patrons); *In re* CVS Caremark Corp., No. C–4259 (F.T.C. June 18, 2009) (disposing of documents containing sensitive medical information in unsecured dumpsters); United States v. Rental Research Servs., Inc., No. 0:09-cv-00524 (D. Minn. Mar. 6, 2009) (failure to implement reasonable procedures to assure that consumer reports are not provided to unauthorized requestors); *In re* Reed Elsevier Inc., No. C–4226 (F.T.C. July 29, 2008) (inadequate security of consumer information stored in databases); *In re* The TJX Cos., Inc., No. C–4227 (F.T.C. July 29, 2008) (inadequate security of personal information collected from retail customers); *In re* CardSystems Sols., Inc., No. C–4168 (F.T.C. Sept. 5, 2006) (inadequate security of information collected from credit card magnetic strips during authorizations); *In re* DSW Inc., No. C–4157 (F.T.C. Mar. 7, 2006) (inadequate security of credit card information collected from retail customers); United States v. ChoicePoint Inc., No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006) (inadequate security of personal information in consumer reports); *In re* BJ's Wholesale Club, Inc., No. C–4148 (F.T.C. Sept. 20, 2005) (inadequate security of credit card information collected from retail customers).

[532] *See, e.g.*, *In re* Carrier IQ, Inc., 78 F. Supp. 3d 1051, 1115–17 (N.D. Cal. 2015) (plaintiffs stated a claim for unfairness under California law against maker of software that was installed on their phones and that allegedly intercepted private information generated through use of their phones and transmitted it to wireless carriers and device manufacturers); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1072–73 (N.D. Cal. 2012) (plaintiffs stated a claim for unfairness under California law against Apple and others for allegedly allowing apps that surreptitiously collected private information to run on their phones); *see also* Assurance of Discontinuance, *In re* Copley Advert., *supra* note 56 (stating view of Massachusetts attorney general that monitoring a phone user's location and sending advertisement to the phone based on its location is unfair under Massachusetts law); Assurance of Voluntary Compliance, *In re* Adobe Sys. Inc. (Nov. 7, 2016) (stating view of attorneys general that failure to maintain reasonable security measures is unfair under law of multiple states) (semble).

*c. The Upshot*

The upshot of these cases is that substantial authority supports the proposition that certain practices invading individual privacy, and the failure to institute reasonable safeguards against unauthorized access to personal information in one's possession, are unfair under the FTC Act and state UDAP laws. Stated another way, legal rules prohibiting unfair *trade* practices, at both the federal and state levels, are available to challenge unfair *privacy* practices. If the goal is to establish *fair* information practice principles, a ban on practices that are *unfair* is a good place to start.

2. Unconscionability

The rule that contracts may be invalidated as "unconscionable" has roots in the common law, originating as a rule of equity.[533] Article 2 (Sales) of the Uniform Commercial Code has included an unconscionability provision, § 2-302, since the original 1952 version of the Code.[534] The current version of § 2-302 reads:

> If the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result.[535]

The UCC does not define the term "unconscionable." The Official Comment to § 2-302 explains, not very helpfully: "The basic test is whether, in the light of the general commercial background and the commercial needs of the particular trade or case, the clauses involved are so one-sided as to be unconscionable under the circumstances existing at the time of the making of the contract."[536] The concept has been characterized as an "amorphous" one that is to be developed on a case-by-case basis so as "to make realistic the assumption of the law that the agreement has resulted from real bargaining between parties who had freedom of choice and understanding and ability to negotiate in a meaningful fashion."[537] An influential gloss on the term as it developed at common law states: "Unconscionability has generally been recognized to include an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party."[538] Consistent with this expression, some courts have operationalized the concept by applying a two-part criterion, requiring that a contract be both procedurally and substantively

533 *See* 8 WILLISTON ON CONTRACTS § 18:1 (4th ed. 2017).

534 U.C.C. § 2-302 (AM. LAW INST. & UNIF. LAW COMM'N 1952).

535 U.C.C. § 2-302(1) (AM. LAW INST. & UNIF. LAW COMM'N 2018).

536 *Id.* § 2-302, cmt. 1.

537 Kugler v. Romain, 279 A.2d 640, 652 (N.J. 1971).

538 Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449 (D.C. Cir. 1965).

unconscionable.[539] Other courts hold that one-sided substantive terms alone can support a decision that the terms are unenforceable because unconscionable.[540]

As developed in the common law and more recently as introduced into state law by enactment of UCC § 2-302, the doctrine of unconscionability applies to contracts. In view of the arguably contractual nature of privacy policies,[541] there is a solid basis for applying unconscionability doctrine in this realm. In addition, unconscionability provisions contained in state UDAP laws are applicable beyond the realm of contracts. Some of these laws specifically prohibit "unconscionable practices," while others treat unconscionable acts as a subset of unfair ones.[542]

*FTC v. VIZIO*, discussed above, illustrates application of the unconscionability doctrine in the privacy context.[543] In that case, the Attorney General of New Jersey was a co-plaintiff along with the FTC. The complaint alleged that VIZIO's undisclosed tracking of consumers' viewing activity was not only unfair under the FTC Act but also that it violated a provision of the New Jersey Consumer Fraud Act forbidding "any unconscionable commercial practice."[544]

### *C. Creating Substantive Standards*

Legislatures, law enforcement bodies, and courts thus have the tools they need to slip the limitations imposed by the procedural approach of notice-and-choice and apply substantive limits to the practices of companies involved in the provision of websites, mobile apps, and IoT devices.

This is not the place for a comprehensive application of these principles to Internet-enabled data flows, which would be a major undertaking. I will content myself here to

---

[539] *E.g.*, Gillman v. Chase Manhattan Bank, N.A., 534 N.E.2d 824, 828 (N.Y. 1988). The meaning of these two terms has been explained as: "Procedural or process unconscionability is concerned with 'unfair surprise,' fine print clauses, mistakes or ignorance of important facts, or other things that mean bargaining did not proceed as it should. Substantive unconscionability is an unjust or 'one-sided' contract." DAN B. DOBBS, 2 LAW OF REMEDIES 706 (2d ed. 1993).

[540] *E.g.*, Maxwell v. Fidelity Fin. Servs., Inc., 907 P.2d 51, 59 (Ariz. 1995).

[541] Several courts have held that the promises contained in a privacy notice may become terms of a contract between the parties to a transaction if all elements can be established. *See* Svenson v. Google Inc., No. 13–cv–04080–BLF, 2015 WL 1503429 (N.D. Cal. Apr. 1, 2015) (plaintiffs stated a claim for breach of contract by violating privacy policy); Smith v. Trusted Universal Standards in Electr. Transactions, Inc., No. 09–4567 (RBK/KMW), 2010 WL 1799456, at *10 (D.N.J. 2010) (no contract claim because plaintiff failed to allege damages flowing from the breach); *In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 325–27 (E.D.N.Y. 2005) (same); *In re* Nw. Airlines Privacy Litig., No. Civ.04–126, 2004 WL 1278459, at *6 (D. Minn. June 6, 2004) (no contract claim because plaintiffs failed to allege several elements). Another court found that privacy policies are generally not contractual, since "broad statements of company policy do not generally give rise to contract claims." Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004).

[542] *See* DEE PRIDGEN & RICHARD M. ALDERMAN, CONSUMER PROTECTION AND THE LAW, § 3:15, at 107–08 ("Fourteen state consumer protection statutes prohibit 'unconscionable' practices. Most of the states that prohibit 'unfair' practices incorporate 'unconscionable' actions as well.").

[543] *See supra* notes 499–504 and accompanying text.

[544] Complaint ¶ 28, *VIZIO*, *supra* note 500 (quoting N.J. STAT. ANN. § 56:8–2); *id.* ¶ 35 (charging VIZIO's conduct as "an unconscionable commercial practice").

propose a single substantive limitation: *There should be a prohibition against conditioning the provision of some good or service on the consumer's consent to the collection and use of her private information that is not required for provision of the good or service. At least this should be so where (a) the good is important to the consumer, and (b) there is only one or only a few sources of the good. Consent to such a practice may only be obtained by an opt-in mechanism including a clear and conspicuous disclosure that consent is optional and that refusing consent results in no penalty*.

If this rule sounds familiar it is because we have encountered it already in the discussion above of what I have termed "gun-to-the-head choice." Several of the policy discussions recommending implementation of the FIPPs have called for such a limitation.[545] Such a limitation was actually implemented in the 1998 COPPA and the (invalidated) 2016 FCC ISP privacy rules.[546] The 2016 GDPR also referenced it favorably.[547] The rule even shows up in voluntary implementations of the FIPPS; for instance, the rules of the Apple App Store prohibit apps from requiring users to submit personal data not needed for the "core functionality" of the app.[548]

A privacy practice of this sort should be prohibited because it deprives the consumer of any actual choice; the choice is merely nominal, masquerading as actual choice. As such, the practice fails to satisfy the widely accepted foundational criterion for what qualifies as a *fair* information practice. As an *unfair* practice, this practice should be banned on the grounds of general principles prohibiting unfair and unconscionable practices.

## VI. CONCLUSION

In this Article, I have argued for rejection of the orthodoxy of notice-and-choice: the idea, enshrined in every version of the fair information practice principles, that the societal interest in protection of information privacy can be vindicated by informing consumers of the uses that a data collector intends to make of their private information and allowing the consumers to choose, on that basis, whether to engage with the information collector. Notice-and-choice could serve this function only in a world where there was no scarcity of consumer time and attention—where rationality was not bounded—and where there was robust competition on privacy terms among suppliers of close substitute goods and services. We do not live in such a world. If we mean to assure that truly fair information practices rule the information ecosystem, rather than merely paying lip service to the notion, we need to move beyond the proceduralist orientation of notice-and-choice and create substantive rules designed to bring about an appropriate balance between the goals of protecting information privacy and allowing societally beneficial uses of private information. Substantive rules in this realm would not be a novelty; such rules exist already, and the principles

[545] The 1973 HEW Report's committee discussions, *see supra* notes 364–66 and accompanying text; the 1977 PPSC report, *see supra* note 367 and accompanying text; the 1995 NTIA white paper, *see supra* text accompanying note 368; and the 2012 FTC report, *see supra* text accompanying notes 370–74.

[546] *See supra* text accompanying notes 475, 478.

[547] *See supra* text accompanying note 377.

[548] *See supra* text accompanying note 328.

underlying the doctrines of unfairness and unconscionability can help us to develop others.