Information Privacy in an Age of Invisible Shopper Tracking: Who Will Pay the Price for Stores of the Future?

Kristin Harripaul
Georgia State University College of Law, kharripaul1@student.gsu.edu

Follow this and additional works at: https://readingroom.law.gsu.edu/gsulr

Recommended Citation
Available at: https://readingroom.law.gsu.edu/gsulr/vol37/iss3/10

This Article is brought to you for free and open access by the Publications at Reading Room. It has been accepted for inclusion in Georgia State University Law Review by an authorized editor of Reading Room. For more information, please contact gfowke@gsu.edu.
INFORMATION PRIVACY IN AN AGE OF INVISIBLE SHOPPER TRACKING: WHO WILL PAY THE PRICE FOR STORES OF THE FUTURE?

Kristin Harripaul

ABSTRACT

Explosive growth in technology has brought a unique opportunity to the doors of brick-and-mortar retail—a nearly $3.38 trillion industry struggling to regain relevance among modern, digitally enabled shoppers. Specifically, in-store analytics, or shopper tracking technologies, are allowing these retailers to better compete with online stores by tapping into consumer data unprecedented in the brick-and-mortar context. With these technologies, stores now have access to detailed metrics, like consumer dwell times, journeys, product engagement, product views, and demographic data such as age and gender, which can be used to optimize store operations and marketing and promotions.

Recent events, however, including a string of data breaches and the passage of strict privacy laws in Europe and California, have renewed efforts for broad information privacy reform that could have deleterious consequences for these technologies. This Note examines the current state of privacy law; two approaches to information privacy reform that appeared before the 116th Congress, namely consumer control and business accountability; and the potential impact of these two regulatory approaches on in-store analytics technologies. It concludes that properly balancing consumer privacy and business interests through regulation requires more than a one-size-fits-all federal band-aid. Instead, it proposes starting with targeted federal acts aimed at the bigger gaps and outliers in existing

* J.D., 2020, Georgia State University College of Law. Special thanks to my faculty advisor, Mark E. Budnitz, Bobby Lee Cook Professor of Law Emeritus at Georgia State University College of Law, for his invaluable guidance and assistance throughout this entire process; Will Bracker, Adjunct Professor of Law at Georgia State University College of Law, for his insightful feedback on this issue; my amazing team from the Georgia State University Law Review for the countless hours spent getting this Note publication-ready; and my family and friends for their undying support and patience.
information privacy law, like brick-and-mortar technologies. Addressing in-store analytics, specifically, it recommends federal regulation focused on business-accountability and expanded FTC powers, and it outlines specific considerations for a targeted act.
CONTENTS

INTRODUCTION ......................................................................................... 1080
I. BACKGROUND .................................................................................... 1084
   A. In-Store Tracking and Related Privacy Concerns ..................... 1087
   B. Protections Under Current Privacy Laws ......................... 1089
II. ANALYSIS ......................................................................................... 1094
   A. The Current Notice-and-Choice Regime ......................... 1097
      1. FTC “Common Law” .............................................. 1098
      2. Implications for Brick-and-Mortar ......................... 1100
   B. Moving Beyond Notice-and-Choice .................................... 1101
      1. Consumer Control Approach .................................... 1102
      2. Business Accountability Approach ............................... 1106
III. PROPOSAL ......................................................................................... 1108
   A. A Uniform Privacy Landscape ............................................. 1109
   B. A Targeted Brick-and-Mortar Technology Privacy Act ... 1111
   C. More Business Accountability and FTC Enforcement ......... 1113
   D. Specific Brick-and-Mortar Considerations .......................... 1116
      1. Fixed, Narrow Definition of PII .................................. 1116
      2. General Duty of Care .............................................. 1118
      3. Reasonable Consumer Control ................................... 1119
CONCLUSION ............................................................................................. 1123
INTRODUCTION

In 2019, the Federal Trade Commission (FTC) made history by imposing a record-breaking $5 billion civil penalty on social media giant Facebook for privacy-related violations.\(^1\) According to the FTC, the penalty “is one of the largest penalties ever assessed by the U.S. government for any violation” and is “almost [twenty] times greater than the largest privacy or data security penalty ever imposed worldwide.”\(^2\) But what even warranted such action, and why are some policymakers saying that the settlement, which includes a twenty-year agreement for independent privacy oversight, still was not severe enough?\(^3\) The answer lies at the heart of a privacy debate that has been brewing in the United States for decades, a debate that grows more complex in an increasingly digital world.\(^4\)

---


3. See, e.g., Dissenting Statement of Commissioner Rohit Chopra at 2, 16, In re Facebook, Inc., No. 182-3109, 2019 WL 3451729, at *2, *16 (F.T.C. July 24, 2019) [hereinafter Dissenting Statement of Commissioner Chopra] (noting that the settlement established a “disappointing precedent” and essentially offered “blanket immunity for unspecified violations by Facebook and its executives,” and that the penalty, although “record-breaking,” did not exceed Facebook’s gains); Dissenting Statement of Commissioner Rebecca Slaughter at 1, 15–16, 19, In re Facebook, Inc., No. 182-3109 (F.T.C. July 24, 2019) [hereinafter Dissenting Statement of Commissioner Slaughter], https://www.ftc.gov/system/files/documents/public_statements/1536918/1536918_3109_slaughter_statement _on_facebook_7-24-19.pdf [https://perma.cc/3G8E-6VED] (emphasizing that the injunctive relief the FTC chose was unlikely to deter Facebook from future violations given that the injunction neither changed Facebook’s fundamental business model nor held Facebook CEO Mark Zuckerberg personally liable, despite signs that the company started violating its original 2012 FTC consent order “early and often”).

4. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 36–37 (2010) (explaining that increasing technological capabilities fueled information privacy debates on the “increasing and potentially unlimited uses of computerized databases of personal information” as early as the 1960s and 1970s); see also Chris Jay Hoofnagle, Archive of the Meetings of the Secretary’s Advisory Committee on Automated Personal Data Systems (SACAPDS): The Origin of Fair Information Practices, BERKELEY L. REV. (reading 1973 transcripts from the committee that...
For a long time, information privacy concerns have focused on cyberspace—social media and e-commerce. But now, a new wave of connected technologies and inexpensive forms of data storage are bringing these concerns to the doors of brick-and-mortar stores, an industry under particular pressure to transform and regain relevance among digitally enabled shoppers. Specifically, growth in in-store analytics—or shopper-tracking technologies, which monitor shoppers’ movements in-store via mechanisms such as video analytics and mobile tracking—is quickly erasing differences between how precisely shoppers can be tracked online and inside a physical store.


7. McKinnon, supra note 5; see also Max, supra note 6 (detailing nineteen different...
For shoppers, the promise of these tracking technologies is a tailored and convenient shopping experience that is more consistent with their online experiences. However, the premise of in-store tracking has left some consumer advocates, academics, and key committee leaders in both the House and Senate uneasy. This uneasiness is further underscored by the fact that these tracking technologies are often invisible to the average shopper. Despite these concerns, however, no uniform information privacy law exists—U.S. privacy law has remained largely self-regulatory and sectoral, unlike many industrialized nations that protect personal data in an omnibus fashion. An array of “constitutional protections, federal and state statutes, torts, regulatory rules, and treaties” regulate different industries and economic sectors, leaving gaping holes with little recourse for these new technology-driven problems.

shopper-tracking mechanisms available in 2020). Video analytics is the use of video sensors placed in stores to collect insights on the shopper—including demographics, in-store journeys, aisle dynamics, category performance, and display optimization, among other metrics—to optimize in-store performance. VideoMining Frequently Asked Questions, VideoMining [hereinafter VideoMining].


8. BRP, Unified Commerce Survey 3 (2019) (finding that 87% of surveyed consumers indicated an interest in a “personalized and consistent experience across all channels”).


10. See Fitzgerald, supra note 6 (explaining that “[p]eople know that they’re being tracked online” but do not realize that the same applies in-store (quoting Pankaj Srivastava, chief operating officer of FigLeaf App Inc.)); see also Soltani, supra note 9; Stephanie Thien Hang Nguyen, What the First Post-Potty Can Teach Designers About Digital Privacy, FAST CO. (Sept. 27, 2019), https://www.fastcompany.com/90409598/what-the-first-post-potty-can-teach-designers-about-digital-privacy [https://perma.cc/K7QS-X5H2] (“Without sights, sounds, and touch, [data privacy] feels practically invisible.”).


12. Id. (“There is a law for video records and a different law for cable records. The Health Insurance
Historically, efforts to create a broad information privacy framework governing how businesses collect, use, share, and protect personal information have struggled to gain traction. But on the heels of the strict online privacy rules established by the 2018 General Data Protection Regulation (GDPR) of the European Union (EU) and the 2019 California Consumer Protection Act (CCPA), privacy advocates and business groups alike are now calling on Congress to create some uniformity amid a growing patchwork of privacy standards. Oddly, despite brick-and-mortar’s control over the majority of consumer sales, its technologies often figure little into narrow, online-focused privacy rhetoric or legislation, and what little guidance does exist leans toward treating online and brick-and-mortar tracking the same.

Portability and Accountability Act (HIPAA) protects the privacy of health data, but a different regime governs the privacy of financial data. In fact, there are several laws that regulate financial data depending on the industry, and health data is not even uniformly protected . . . .” (footnotes omitted)).


14. Grande, supra note 13 (“The U.S. Chamber of Commerce, the Internet Association and BSA: The Software Alliance, along with tech giants such as Google, Microsoft and Apple, are among the stakeholders in the business community that have recently thrown their support behind . . . uniform . . . privacy rules, with several offering up their own proposed frameworks.”).

15. JOSEPH TUROW, THE ASILES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY, AND DEFINE YOUR POWER 8 (2017) (“Oddly, although these [in-store tracking] practices relate to the ongoing and widespread public discussion about privacy . . . retailers only barely figure in the debate. The shopping aisle has, in fact, received almost no attention even among academics.”); see also BUREAU OF THE CENSUS, U.S. DEP’T OF COM., CB20-24, QUARTERLY RETAIL E-COMMERCE SALES 4TH QUARTER 2019, at 2 tbl.1 (2020) (noting that brick-and-mortar sales accounted for approximately 89% of total retail sales in 2019); David F. McDowell et al., What the Nomi Case Could Mean for Retail Tracking, LAW360 (May 19, 2015, 10:10 AM), https://www.law360.com/articles/655958/what-the-nomi-case-could-mean-for-retail-tracking (noting that based on the FTC’s first settlement against a retail tracking company, “it is reasonable to anticipate that the FTC will move in a direction that mirrors its position with respect to online tracking . . . .”).
As such, in-store tracking technologies could be one of the first casualties of new privacy reform laws, hampering the brick-and-mortar retailer’s ability to compete in an increasingly complex and digital world. The following Note discusses how policymakers should address shopper-tracking practices in brick-and-mortar amidst prompts for privacy reform. Part I examines key in-store tracking practices and concerns and the current state of privacy law. Part II analyzes various bills and proposals, from privacy advocates and business groups alike, for privacy reform. Part III proposes specific considerations to balance privacy rights against support for the next phase of brick-and-mortar innovation—the store of the future.

I. BACKGROUND

Over the last decade, explosive growth in technology has changed the rules of engagement, providing businesses with access to massive pools of data across almost every aspect of consumers’ lives. These technologies have built a rich digital economy and left a trail of electronic breadcrumbs that businesses, under competitive pressures, are driven to turn into profit. Furthermore, in an intriguing paradox,

16. Keyes, supra note 9 (“Any future regulations dealing with in-store data privacy will likely hamper physical retailers' ability to provide a personalized and convenient shopping experience. If retailers’ ability to identify and track consumers in-store is restricted, they may struggle to personalize in-store shopping.”); see also McKinney, supra note 5 (“Privacy legislation is drawing concern from traditional retailers who worry that their cutting-edge technologies could be banned or disrupted if they are included under the privacy law.”).


18. See Jeff Jonas, The Surveillance Society and Transparent You (explaining that organizations of all shapes and sizes must have access to more information and make sense of it if they hope to survive), in PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS, supra note 17, at 93, 94; see also Press
consumers have been willing contributors to this digital economy despite mistrusting companies that monitor their behavior. They confess their problems on social media, allow apps to track their mobile location, and welcome an increasing number of smart technologies into their lives in exchange for convenience and other value. As a result, industry experts estimate that this digital economy is “doubling the volume of information in the world every two years.”

This nonstop disruption has shaken up the very foundation of retail, “creating opportunities for new entrants, and making transformation an imperative for [brick-and-mortar] incumbents” that are sorely ill-prepared for this digitally enhanced marketplace.

See Brooke Auxier et al., Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information, Pew Rsch. Ctr.: Internet & Tech. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (highlighting that “a majority of Americans report being concerned about the way their data is being used by companies (79%) . . . ”); see also Tal Z. Zarsky, Privacy and Manipulation in the Digital Age, 20 Theoretical Inquiries L. 157, 162 (2019) (highlighting that “contrary to several surveys indicating a consumer preference toward privacy,” consumers’ “constant tendency to waive their data-related rights” indicates a disinterest in control and that consumers’ preferences and interests lie elsewhere).


Modern shoppers—with increased access to information and growing expectations—have created a nightmare of a moving target for traditional retail stores that rely on limited transactional and loyalty data with little visibility into shopper behavior and what shoppers actually experience inside the physical environment.23 Additionally, because extracting insight from these traditional sources has minimal effect on daily decision making, brick-and-mortar retailers have little means to control their bottom line by adjusting and improving the shopping experience in real-time.24

As such, analysts believe the retail industry is at “a major inflection point.”25 Unsurprisingly, brick-and-mortar “retailers are increasingly turning to data and analytics,” with shopper-tracking being the number one technology on retailers’ list of technology-enabled growth strategies for 2021.26 With everything to lose, brick-and-mortar is now looking to join the race to turn shopper data into a meaningful business advantage before online players


23. See SHOPPER TECH. INST., DIGITAL DISRUPTION IN CPG & RETAIL loc. 198 (2018) (ebook) (“Current analytical models based on spend data only with limited customer information are unable to predict shopper interests and purchases.”); see also Karsten & West, supra note 22 (explaining how online retailers “can gather customer data with every click and then rapidly redesign their website to boost sales, [while] brick-and-mortar stores might only track final purchases”); Rajeev Sharma, Adapting to the New Cherry-Picking Shopper, WALL ST. J. (Nov. 24, 2014, 7:57 PM), https://www.wsj.com/articles/it-wont-be-easy-making-money-off-of-cherry-picking-shoppers-1416877025 [https://perma.cc/Z3K4-MYFC] (explaining how modern, cherry-picking shoppers are “spoiled for choice” and “won’t be very lucrative unless stores adapt”); VideoMining, supra note 7 (discussing the limits on the sales and loyalty card data brick-and-mortar already holds).

24. Terry, supra note 6 (describing the store floor as a “previously data-dark place”); see also RETAIL WIRE RSCH., HOW SHOPPER INSIGHTS ARE FUELING RETAIL PROGRESS 2 (2014) (finding that 84% of brick-and-mortar incumbents describe themselves as “newbies” and “getting there” in harnessing their data); SIDES & FURMAN, supra note 22, at 14 (“For years, the industry struggled with how to create and use data.”). See generally Jia Wertz, Why Brick and Mortar Retailers Need E-Commerce-Style Data Tracking Methods, FORBES (Dec. 18, 2017, 5:15 PM), https://www.forbes.com/sites/jiawertzt/2017/12/18/brick-and-mortar-retailers-need-e-commerce-style-data-tracking/#7f562f9280eb [https://perma.cc/U9D9-3RVZ] (indicating that brick-and-mortar data has been very difficult to access and turn into actionable insight for use in daily decision-making processes).

25. Sides & Furman, supra note 22, at 3; see also Max, supra note 6.

render stores obsolete. Despite a general lack of agility, budgetary barriers, and legacy system integration problems, already 11% of retail stores have adopted in-store tracking technologies, and 41% plan to invest in shopper tracking capabilities for 2021.

A. In-Store Tracking and Related Privacy Concerns

The desire to collect data on shoppers is not a new practice; retailers have been doing it for decades. But now, retailers like Walmart, Target, Macy’s, Nordstrom, Cabela’s, and many more are building stores of the future and gathering new categories of consumer behavioral data through a variety of methods.

In particular, retail stores are beginning to tap into data unprecedented in the brick-and-mortar context, with in-store tracking technologies, like video and mobile analytics that monitor consumers through the use of video and cellphone signals. With these technologies, physical stores have access to many of the analytics already available to online stores, including traffic counts, in-store journeys, product engagement, products viewed, dwell times, and demographic data such as gender and age range. These metrics can be used to optimize layout and store planning, staffing and merchandising, and marketing and promotions.

27. Jonas, supra note 18; see also SIDES & FURMAN, supra note 22; SKORUPA, supra note 26; Moreno, supra note 22.
31. See, e.g., Clifford & Hardy, supra note 30 (highlighting the use of video and mobile tracking to learn gender, time spent in certain aisles, and time spent looking at specific merchandise); see also Terry, supra note 6.
32. McKinnon, supra note 5; Terry, supra note 6; Max, supra note 6.
33. Terry, supra note 6; Anne Stephen, Finding the ROI in Retail In-Store Analytics, STREET FIGHT
The type of data collected from these tracking devices varies from one solution and provider to the next, but generally, the data collected is labeled as either personal information, also known as personally identifiable information (PII), or nonidentifiable information.\textsuperscript{34} PII is commonly used to describe information that uniquely identifies a shopper, typically by name, whereas nonidentifiable information does not identify the shopper and is not considered linkable to that specific shopper.\textsuperscript{35} Notably, these neat labels often offer a fictitious distinction given the “messiness” and “malleable nature” of big data and the fact that nonidentifiable data can increasingly be reidentified as technology advances.\textsuperscript{36}

In brick-and-mortar, as well as online, the ability to aggregate different data sets and thereby generate additional consumer information beyond the limits of provided data sets is a key concern with tracking technologies.\textsuperscript{37} The idea is that, under the guise of promised benefits like “convenience,” companies aggregate expansive amounts of consumer data to construct precise personality, psychological, and behavioral profiles in an effort to automate buying behavior and essentially erode personal choice.\textsuperscript{38}

\textsuperscript{34} See Paul M. Schwartz & Daniel J. Solove, Reconciling Personal Information in the United States and the European Union, 102 CALIF. L. REV. 877, 878–79 (2014); see also Max, supra note 6.

\textsuperscript{35} Max, supra note 6; Schwartz & Solove, supra note 34, at 879.

\textsuperscript{36} See Christopher Wolf, Envisioning Privacy in the World of Big Data, in PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS, supra note 17, at 204, 208; see also Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. REV. 1814, 1841–45 (2011) (describing means by which data can become identifiable); Soltani, supra note 9 (looking specifically at how information gathered via mobile analytics techniques can become identifiable); Deborah Hurley, Taking the Long Way Home: The Human Right of Privacy (explaining that the combination of the Internet of Things and nascent big data may make it challenging to maintain anonymity), in PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS, supra note 17, at 70, 76.

\textsuperscript{37} NISSENAUB, supra note 4, at 43; SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 8 (2019); Altshuler, supra note 4.

\textsuperscript{38} ZUBOFF, supra note 37; Altshuler, supra note 4; see also Drew Harwell & Abha Bhattarai, Inside Amazon Go: The Camera-Filled Convenience Store That Watches You Back, WASH. POST (Jan. 22, 2018, 6:00 PM), https://www.washingtonpost.com/news/business/wp/2018/01/22/inside-amazon-go-the-camera-filled-convenience-store-that-watches-you-back/ [https://perma.cc/X5C8-P3B2] (examining the cashierless Amazon Go store and explaining that powerful companies like Amazon have more than just data on a shopper’s purchases—"‘they’re also connected with . . . nearly every aspect of [the shopper’s] life,” including where people live and what they buy, read and watch,” which all feed into a shopper’s
Privacy advocates also argue that these superpowered profiles open the door for automated discrimination, whereby shopper profiles deemed most profitable receive tailored deals, different pricing, and better service than consumers on the less profitable end of the spectrum. Likewise, minorities and other groups could also receive disparate treatment based on data collected. Another big concern is that as these technologies become more powerful, they also become more inconspicuous or invisible to shoppers: they are embedded in the phones they carry or in shelves, ceilings, and other areas throughout the shopping experience.

B. Protections Under Current Privacy Laws

Despite changing societal norms and the advent of the “oversharing economy,” or the “era of revelation,” there appears to be a broad agreement that privacy is not a dead issue and still deserves protection, according to privacy professor and expert Anita Allen. However, as it stands, the Constitution does not explicitly

---

41. See Terry, supra note 6; Soltani, supra note 9; see also NISSENBAUM, supra note 4, at 23 (“[T]he trend is toward systems of networked sensors that are so small as to be imperceptible by humans, some on the nanoscale.” (citation omitted)); see also Hurley, supra note 36 (“Much of . . . information activity will happen outside the limits of human sensory and temporal awareness.”); Schneier, supra note 17 (noting that “ubiquitous surveillance is not only possible but cheap and easy”). See generally How it Works, RETAILNEXT, https://retailnext.net/en/how-it-works/ [https://perma.cc/HTZ2-R7CC] (providing an example of the power of a retail analytics platform and the wide variety of sources that can already be aggregated).
42. See Anita L. Allen, Lecture, What Must We Hide: The Ethics of Privacy and the Ethos of Disclosure, 25 ST. THOMAS L. REV. 1, 1, 5, 18 (2012) (describing the “era of revelation” as an era heavily influenced by technology and marked by individual preoccupation with “broadcasting what we know, think, do, and feel” and noting a developing indifference to privacy); Toby Daniels, How Overenthusiasm for Tech Led to an Era of Oversharing and Data, ADWEEK (Apr. 4, 2018), https://www.adweek.com/performance-marketing/how-overenthusiasm-for-tech-led-to-an-era-of-oversharing-and-data-scandals/ (observing a shift in consumer infatuation with social media and explaining how “[o]versharing became the new normal”); see also, e.g., In re Facebook, Inc., 402 F. Supp. 3d 767, 776 (N.D. Cal. 2019) (rejecting vehemently Facebook’s views that social media users cannot reasonably expect their personal information and communications to remain private, even after sharing with friends, writing: “Facebook’s argument could not be more wrong”); Birnbaum, supra note
grant a right to privacy, and neither a single plenary data protection regulator nor a single definition of PII, which triggers the application of privacy law, exists. Instead, privacy laws are largely a sectoral hodgepodge of differing governmental views on consumers’ rights, leaving several unregulated gaps. At the federal level, for instance, no law directly regulates data collection and use by companies such as Facebook and Google, let alone brick-and-mortar retailers. Further, in comparison to the European Union and other industrialized nations, privacy standards in the U.S. have been described as “fragment[ed] and hollow,” providing few limits on data collection, use, and disclosure.

Accordingly, the FTC, which stepped in to mitigate this void in the early nineties, has become the broadest and most influential protector of information privacy in the U.S.—more so than any privacy statute


43. See NISSENBAUM, supra note 4, at 238; Natasha Singer, The Government Protects Our Food and Cars. Why Not Our Data?, N.Y. TIMES (Nov. 2, 2019), https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html [https://perma.cc/L9MM-XW6R] (“The United States is virtually the only developed nation without a comprehensive consumer data protection law and an independent agency to enforce it.”); Doug Linder, The Right of Privacy, EXPLORING CONST. CONFLICTS, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html [https://perma.cc/TH7W-ZEUA] (exploring in detail whether the Constitution protects the right to privacy); Schwartz & Solove, supra note 36, at 1816, 1826–27 (arguing that PII is one of the most important concepts in privacy regulation because numerous state and federal statutes rely on its distinction and share the basic assumption that in the absence of PII, no privacy harm exists).

44. NISSENBAUM, supra note 4, at 238; Solove & Hartzog, supra note 11; see also Natasha Singer, The Week in Tech: Why Californians Have Better Privacy Protections, N.Y. TIMES (Sept. 27, 2019), https://www.nytimes.com/2019/09/27/technology/the-week-in-tech-why-californians-have-better-privacy-protections.html [https://perma.cc/7RA4-HR57]. Privacy advocates criticize a “sectoral” approach because they contend that there is no express right to privacy in the Constitution or legislation, and privacy is thus viewed as a preference that may be lightly bartered off according to competitive free market norms. NISSENBAUM, supra note 4, at 237–38. Instead, privacy advocates tend to prefer an “omnibus” approach because it is seen as recognizing privacy as a fundamental human right that cannot be bartered off due to an overarching national commitment to privacy constraints detailed in legislation. Id.

45. Solove & Hartzog, supra note 11.

46. Id. at 586–87; Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in Ratcheting Up of U.S. Privacy Standards, 25 YALE J. INT’L L. 1, 23 n.82 (2000); Singer, supra note 43; see also Hurley, supra note 36, at 74 (noting that, unlike other countries, the U.S. has failed to keep up as information and communication technologies have advanced, leaving Americans with fewer protections for their personal data).
or common law tort.\textsuperscript{47} In fact, “[t]oday, the FTC is viewed as the de facto federal data protection authority.”\textsuperscript{48} However, because the FTC cannot practically set substantive privacy rules or generally impose penalties unless an entity has violated an existing FTC order, it has acted primarily as an enforcer, proceeding under a general grant of authority grounded in section 5(a) of the FTC Act, which prohibits “unfair or deceptive acts or practices.”\textsuperscript{49}

Under this framework, a rich collection of over 500 enforcement FTC actions related to consumer privacy have been likened to privacy “common law” by Professors Daniel Solove and Woodrow Hartzog.\textsuperscript{50} Moreover, the understanding of “unfair or deceptive acts” has expanded to include not only a failure to comply with published privacy promises, but also a general theory of deception with respect to obtaining personal information and providing insufficient notice of

\begin{flushright}
\textsuperscript{47} Marc Rotenberg, \textit{EPIC: The First Twenty Years} (describing how the Electronic Privacy Information Center (EPIC), a privacy interest group, turned to the FTC to strengthen privacy regulation amid a “patchwork of law . . . emerging in the United States in the early 1990s that seemed inefficient and incoherent”), in \textit{PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS}, supra note 17, at 10, 10–11; Solove & Hartzog, supra note 11.

\textsuperscript{48} Solove & Hartzog, supra note 11, at 600. The FTC was originally created in 1914 with the intent to “ensure fair competition in commerce,” but “[a]t the urging of Congress” and privacy interest groups in 1995, “the FTC became involved with consumer privacy issues.” \textit{Id.} at 598; Rotenberg, supra note 47, at 11; \textit{Our History, FED. TRADE COMM’N}, https://www.ftc.gov/about-ftc/our-history [https://perma.cc/BV6Y-DRKC].


\textsuperscript{50} Solove & Hartzog, supra note 11, at 619, 621, 622–23 (arguing that privacy-related settlements the FTC issues are the functional equivalent of privacy common law, much like bodies of case law, given their publicized nature, precedential treatment by privacy practitioners, and consistency); FED. TRADE COMM’N 2017, supra note 49, at 2.
This privacy oversight is largely recognized as the notice-and-choice regime and offers much counsel for online practices. Notably absent from this oversight, however, is counsel within the specific context of brick-and-mortar technology—to date, only one FTC settlement has addressed in-store tracking. Without prescriptive regulations, businesses face uncertainty in navigating whether conduct falls within a safe harbor and are therefore forced to interpret FTC actions and guidance for “compliance nuggets.”

Questions as to the actual scope of the FTC’s powers have further muddied the waters. Meanwhile, at the state level, most privacy and tort laws have historically been ineffective at addressing these emerging digital problems. But because of little progress made on a federal law, many states have started taking matters into their own hands.

---

51. Solove & Hartzog, supra note 11, at 627–43 (providing an in-depth analysis of FTC privacy jurisprudence over “unfair or deceptive acts”).
52. See id. at 592.
55. See, e.g., F.T.C. v. Shire Viropharma, Inc., 917 F.3d 147, 160–61 (3d Cir. 2019) (narrowing the time frame that the FTC can investigate and bring cases under its section 13(b) powers by finding that the FTC could not state a claim after a five-year gap had lapsed between when the alleged misconduct ended and when the FTC filed its complaint).
56. Solove & Hartzog, supra note 11, at 587–88. Technology has outpaced conceptions of privacy and foreclosed application against retail stores because courts remain unwilling to extend expectations of privacy to public spaces and continue to find that privacy does not exist if the information has been either exposed to the public or disclosed to others. Vincent Nguyen, Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 560–61 (2019).
California, in particular, has already developed one of the most comprehensive privacy measures in the United States after the bill raced through the state legislature with grudging support to avoid an even tougher ballot initiative. The CCPA essentially grants consumers an exclusive right to privacy regarding all of their personal information. Like the GDPR, which recognizes privacy and the protection of personal data as fundamental human rights, the CCPA provides strong protections for consumers.

The recently passed California Privacy Rights Act, which amends the CCPA and takes effect in January 2023 with a “look back” to January 2022 for enforcement purposes, expands protections even further.

Without a national privacy law, the GDPR and the hastily passed CCPA have become the new face of information privacy legislation, with many states pushing to introduce mirror legislation. However, the costs of compliance and risk of error in navigating fifty unique state laws along with any applicable federal and foreign laws could

---


59. See CAL. CIV. CODE § 1798.100 (West 2020) (providing a right to request disclosure of personal information collected); id. § 1798.105 (providing a right to request deletion of information collected); id. §§ 1798.110, .115 (providing a right to request disclosure of personal information sold to third parties); id. § 1798.120 (providing a right to request that personal information not be sold to third parties); id. § 1798.140.

60. Wakabayashi, supra note 58.


62. See Wakabayashi, supra note 58 and accompanying text; Rippy, supra note 57; Stone, supra note 57 (citing California Senator Bob Hertzberg describing the states stepping in on marijuana legislation because of the size and slow-moving nature of the federal government as an apt analogy for privacy rights); Grande, supra note 13. See generally Serrato et al., supra note 42.
create a nightmare for some businesses.\textsuperscript{63} Multiple conflicting laws would also create confusion and inconsistent outcomes for consumers as they shop locally, online, and across the country.\textsuperscript{64} Stricter online protections also raise additional questions about how these laws would apply to brick-and-mortar.\textsuperscript{65} In-store tracking technologies remain unaddressed in current legislation and barely figure into current debates, despite brick-and-mortar control of 84% of all retail sales, even during the COVID-19 pandemic.\textsuperscript{66} As such, a dire need for more uniform direction concerning information privacy exists, particularly in the brick-and-mortar context.\textsuperscript{67}

II. ANALYSIS

Thanks to pressure from the GDPR and the CCPA, for the first time, there is a general consensus among Congress and both consumer and business interest groups alike that a national privacy law is well-founded.\textsuperscript{68} To this end, more than a dozen bills and
discussion drafts targeting more comprehensive online privacy reform were circulated in the 116th Congress.\(^6^9\) To advance this dialogue, other members of Congress, along with privacy advocacy organizations and businesses, also offered model legislation drafts and policy frameworks, and congressional committees held a handful of privacy-related government hearings.\(^7^0\)

Although none of these items individually may anticipate the contents of a final federal act, collectively they mark the contours of the chief issues moving into the next congressional session. Accordingly, a review of these materials first reveals broad support for increased consumer privacy protections beyond the current government to save them from the states); Comment Letter from Nicholas R. Ahrens, Vice President of Priv. & Cybersecurity, Retail Indus. Leaders Ass’n, to Nat’l Telecomms. & Info. Admin. (Nov. 9, 2018) [hereinafter RILA Comment Letter], https://www.ntia.doc.gov/files/ntia/publications/rila_ntia_privacy_comment_final.pdf [https://perma.cc/32NT-LRE7] (agreeing with the need for a uniform standard).


notice-and-choice model. A closer look, however, specifically at the bills and proposals introduced in the 116th Congress, betrays bipartisan consensus on several key issues.

For example, most congressional members agree on the need for a federal privacy regulator. Although some would appoint the FTC, others are unconvinced of the FTC’s fitness, perhaps siding with critics on the FTC’s “inadequacy and toothlessness” and past of “rampant regulatory overreach” when it held broad authority to issue substantive rules. The bills and proposals would also generally minimize data collection and put information safeguards in place. Additionally, despite PII’s conceptual problems, lawmakers in the 116th Congress widely agreed that some concept of PII is necessary moving forward.

More significantly, a number of the bills and proposals approach privacy reform by concentrating on strengthening consumer control of data, similar to the CCPA, albeit with variances on the types of

71. See, e.g., S. 3300, § 2 (noting that increasing digitalization of information has magnified the harm to individual privacy and as such it is necessary for Congress to act); Fact Sheet: Chairman Wicker’s Discussion Draft the United States Consumer Data Privacy Act, U.S. SENATE COMM. ON COM. SCI. & TRANSP. (Dec. 3, 2019), https://www.commerce.senate.gov/2019/12/chairman-wicker-s-discussion-draft-the-united-states-consumer-data-privacy-act [https://perma.cc/J2XM-56WX] (explaining that the twenty-first-century American economy is increasingly driven by data, leading to numerous high-profile misuses of data, for which consumers have demanded Congress step in); SENATE DEMOCRATS, supra note 70 (emphasizing that basic legal frameworks protecting privacy have not evolved to meet the new reality of technology and data collection); see also Cameron F. Kerry, Breaking Down Proposals for Privacy Legislation: How Do They Regulate?, BROOKINGS (Mar. 8, 2019), https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate [https://perma.cc/L6YJ-DQL2] (showing that notice-and-choice is widely viewed as insufficient among privacy mavens).

72. See S. 2637, § 8 (creating a “Bureau of Technology” within the FTC); S. 142, § 5 (naming the FTC as the federal privacy regulator); S. 3456, § 9 (naming the FTC as the federal privacy regulator); Birnbaum, supra note 40 (creating a bureau within the FTC). But see S. 3300, § 4(a) (establishing a “Data Protection Agency” instead); H.R. 4978, § 301 (establishing an independent “United States Digital Privacy Agency” instead).


74. See, e.g., S. 3456 §§ 3(d), 6 (including specific data minimization and data security provisions); S. 2968 §§ 106, 107 (same); H.R. 4978, §§ 201, 214 (same); S. 1214 §§ 12, 13; USCDPA, supra note 69, at 10–11, 17–18 (same).

75. Schwartz & Solove, supra note 36, at 1828; see also, e.g., S. 3300 § 3(5); S. 3456 § 2(9); S. 2968 § 2(8); S. 2637 § 2(12); H.R. 4978 § 2(13).
controls given to consumers. This approach contrasts with the business accountability approach that businesses and organizations advanced in their policy frameworks and in the provisions of drafts like the United States Consumer Data Privacy Act (USCDPA). Notably, the deceptively subtle differences between these two approaches could present very different outcomes for brick-and-mortar tracking technologies.

Perhaps the biggest privacy reform battles in the 116th Congress, however, took shape in a category privacy expert Cameron Kerry labeled as “end game issues,” which he argues “are too politically charged to resolve without a clear picture of the substance of privacy protection in a bill.” These issues include private rights of action and preemption of state laws. Preemption is of particular concern in brick-and-mortar privacy rhetoric.

A. The Current Notice-and-Choice Regime

When the FTC first stepped onto the privacy scene in 1995, it embraced the existing scheme of industry self-regulation out of “fear that regulation would stifle the growth of online activity.” Under this scheme, businesses essentially determined for themselves the basic rules they would adhere to regarding data collection, use, and...

---

76. See sources cited supra note 59; see also S. 2968 §§ 102–05, 204(b) (providing a private right of action and base consumer rights of access, correction, deletion, portability, and information); H.R. 4978 §§ 102–09, 407 (providing the same with additional consumer rights of human review of automated decisions, information, impermanence, and individual autonomy); S. 3456 §§ 4–5 (providing individual consumer rights of access, portability, and information but no private right of action); S. 1214 §§ 4–6, 17 (providing a private right of action and base consumer rights); USCDPA, supra note 69, at 7–10 (providing base consumer rights but no private right of action).

77. See CDT FEDERAL BASELINE, supra note 70; Intel Legislation, supra note 70; USCDPA, supra note 69; see also Developing the Administration’s Approach to Consumer Privacy, 83 Fed. Reg. 48,600, 48,600–01 (Sept. 26, 2018) (proposing a shift away from mandating notice-and-choice to focusing on outcomes of organizational practices in 2018).

78. See generally discussion infra Section II.B.


80. Id.

81. NRF Comment Letter, supra note 67; RILA Comment Letter, supra note 68, at 3.

82. Solove & Hartzog, supra note 11, at 598.
disclosure; businesses then stated the rules in privacy policies. This self-regulatory privacy regime has largely continued under the FTC but now “with some oversight,” relying on notice and choice as key aspects of enforcement.

The use of privacy policies arose out of the Fair Information Practices (FIPs), first stated in a 1973 U.S. Department of Health, Education, and Welfare (HEW) report and later expanded by the Organization for Economic Cooperation and Development (OECD) in its 1980 privacy guidelines. The HEW report emerged as a response to the widespread use of automated data systems containing personal information, like social security numbers, in both the public and private sectors. Individuals’ right to notice about the collection and use of their data, and right to consent to this collection and use, were two of the most prominent FIPs and thus “became the backbone of the U.S. self-regulatory approach.”

1. FTC “Common Law”

Initially, FTC oversight consisted mainly of adding some teeth to privacy policies, most of which lacked any penalty or consequence if a company failed to live up to its promises. This oversight has since grown into some general parameters around the notice-and-choice requirement. Vague language, technically correct but incomplete language, and language hidden in dense boilerplate policies have all been deemed insufficient for notice purposes.

Further, even if no notice is given, and thus no promise is broken, the FTC has taken a stance against surreptitious consumer
surveillance online.\textsuperscript{91} In \textit{In re Aspen Way Enterprises, Inc.}, the FTC found that installing spyware and gathering data without notice was an unfair practice.\textsuperscript{92} Although the FTC did not allege in its complaint that Aspen Way made any privacy-related promises, the FTC deemed the surreptitious data gathering unfair due to the substantial harm caused to consumers from such invasive surveillance and concerns that “[c]onsumers [could not] reasonably avoid these injuries because [the surveillance was] invisible to them.”\textsuperscript{93}

In the specific context of brick-and-mortar tracking, the FTC has handled only one case.\textsuperscript{94} In \textit{In re Nomi Technologies, Inc.}, the FTC found that shopper tracking in brick-and-mortar can also be deceptive if consumers are not adequately informed of these activities.\textsuperscript{95} Specifically, the FTC found that Nomi’s representations in its privacy policies that consumers were “always” allowed to opt-out of its mobile tracking services were deceptive because an opt-out mechanism was available online but not in-store and because consumers were given no notice that they were being tracked at a retail location.\textsuperscript{96}

However, several issues take shape in \textit{In re Nomi}.\textsuperscript{97} Although Nomi failed to offer an in-store opt-out as promised in its privacy policy, Nomi was not even required to offer such an option because it did not collect PII.\textsuperscript{98} Yet, for this single misstatement, which went beyond minimum standards, the FTC gave Nomi (a small, two-year-old start-up) the same punishment as Facebook (a

\textsuperscript{91} Id. at 641.

\textsuperscript{92} See Complaint at 4, \textit{In re Aspen Way Enters., Inc.}, FTC File No. 112-3151 (F.T.C. Apr. 11, 2013) (No. C-4392) [hereinafter Aspen Complaint]; see also Solove & Hartzog, supra note 11, at 641.

\textsuperscript{93} Solove & Hartzog, supra note 11, at 641 (quoting Aspen Complaint, supra note 92, at 2).

\textsuperscript{94} Retail Tracking Firm, supra note 53.


\textsuperscript{96} Id.


\textsuperscript{98} Dissenting Statement of Commissioner Wright, supra note 97, at 1 (explaining that Nomi neither tracked individual consumers nor identified them); Sparapani, supra note 97.
multibillion-dollar company) despite little, if any, economic consumer injury.\textsuperscript{99}

2. Implications for Brick-and-Mortar

The puzzling result in \textit{In re Nomi} reflects an immediate need for greater penalty gradations and for more definition as to what constitutes an “injury” outside of economic harms.\textsuperscript{100} More importantly, it also highlights deeper issues concerning the practicality of the notice-and-choice regime and the FTC’s intention to apply it to in-store technologies, given that the FTC did not order any affirmative notice-and-choice obligations.\textsuperscript{101}

The \textit{In re Nomi} decision is also particularly troubling given brick-and-mortar retail’s painful three-dimensional constraints that significantly stunt speed-to-market.\textsuperscript{102} For example, a simple graphic update on a merchandising display involves meticulous planning and project management to ensure the signage is printed, shipped, and installed in compliance with merchandising standards.\textsuperscript{103} Depending on the company’s approval process, the number of stores and differing store layouts, and the complexity of the project, this process could take weeks.\textsuperscript{104} As such, it is unsurprising that bigger

\textsuperscript{99} Dissenting Statement of Commissioner Wright, \textit{supra} note 97, at 4 (describing Nomi’s failure as a “minor shortcoming” and stating that “there [was] no evidence the misrepresentation harmed consumers”); Sparapani, \textit{supra} note 97.

\textsuperscript{100} See Sparapani, \textit{supra} note 97.

\textsuperscript{101} Dissenting Statement of Commissioner Wright, \textit{supra} note 97, at 1 (pointing out that even if the facts of the \textit{In re Nomi} case did support a technical violation, prosecutorial discretion favored restraint); McDowell et al., \textit{supra} note 15 (noting that the FTC’s approach in \textit{In re Nomi} “raises the question of whether the FTC would ever impose a notice and choice obligation for offline, retail tracking” and provides “no certainty around the FTC’s view”); Sparapani, \textit{supra} note 97 (hypothesizing that the effects of the \textit{In re Nomi} order are “likely” to extend to all businesses).

\textsuperscript{102} See NISSENBAUM, \textit{supra} note 4, at 29.


\textsuperscript{104} See, \textit{e.g., THE VOMELA COS., PETCO DOG TREAT PROJECT 2, https://cdn2.hubspot.net/hubfs/1689179/Case20Studies/Petco/VOM-MKT_Petco_Case-Study_V2.pdf} [https://perma.cc/5B8W-DE9W] (detailing a case study on how updating simple merchandising graphics across 1,400 Petco stores took four weeks, not including the approval process).
store-of-the-future concepts are tested in innovation labs, with rollouts taking place years later.\(^{105}\)

Looking specifically at in-store tracking technologies, a national rollout, along with shipping and installation, requires mapping analytics objectives against measurable key performance indicators of the technology.\(^ {106}\) It also includes numerous site visits to understand differing store layouts, determine hardware placement, evaluate adaptions for legacy systems, and test the technology.\(^ {107}\) In this challenging three-dimensional store environment, a lack of certainty and fear of facing government fines or penalties inhibits already slow adoption and growth rates in innovative technologies, during a very competitive time.\(^ {108}\) Although FTC oversight and the notice-and-choice regime have offered some aid for companies wrestling with data innovation and privacy, much uncertainty still remains for brick-and-mortar.\(^ {109}\)

**B. Moving Beyond Notice-and-Choice**

As the notice-and-choice regime continues to receive scrutiny, two key regulatory approaches appear in information privacy reform discussions: one focusing on consumer control and one focusing on business accountability.\(^ {110}\)

---


107. Id.


110. See Kerry, *supra* note 71 (making a similar finding and referencing the two privacy models as consumer choice and business behavior); see also GDPR & CCPA: Opt-Ins, Consumer Control, and the
1. Consumer Control Approach

The idea behind the first approach to privacy reform, followed by a number of privacy bills and proposals before the 116th Congress, is that the appropriate response to increased data pooling is increased consumer control of data. Advocates flock to this property-style model because it is seen as offering consumers the greatest protections and recognizing privacy more or less as a fundamental right. This is the premise behind the GDPR, the CCPA, the CPRA, and bills like the Data Protection Act of 2020 and the Consumer Online Privacy Rights Act.

Under this approach, privacy cannot be left to self-regulation when businesses have such substantial profit incentives. These models attempt to place consumers squarely in the driver’s seat with exclusive control of their personal data, frequently including some form of a private right of action (PRA) for consumers.
Many of these models continue to rely heavily on notice and consent before or during collection of PII, with limited exemptions. The CPRA has gone so far as to require that any consent given must be “freely given, specific, informed and unambiguous,” and one bill requires affirmative consent even for aggregated personal information used for behavioral personalization, offering an exemption only for the strict purpose of increasing usability for the benefit of the consumer.

Additionally, although one bill proposed setting a minimum percentage of individuals who must read and understand a notice or consent process, the bill, like its counterparts, fails to address problematic privacy policy and notice-delivery mechanisms in any meaningful way. Instead, the bills and proposals focus on arming consumers with a core set of individual rights, such as the rights of access, correction, deletion, portability, and information.

In defining PII, these models lean toward a more expansive definition. A number of the bills and proposals defined PII as information “linked or reasonably linkable” to an individual or device. According to Professors Paul Schwartz and Daniel Solove, this broad standard allows for flexibility in adapting to new technological developments, unlike provisions that merely enumerate


117. MacTaggart Letter, supra note 113, at 22; H.R. 4978 §§ 106(b), (d).

118. See, e.g., H.R. 4978 § 213(d) (providing only that notice “shall be (A) clear and in plain language; and (B) made publicly available in a prominent location on an ongoing basis . . . and shall be made available . . . before any collection of personal information”).


120. See, e.g., H.R. 4978 § 2(13)(A)–(B) (defining PII as “any information maintained by a covered entity that is linked or reasonably linkable to a specific individual or a specific device, including de-identified personal information” (emphasis added)); S. 3456 § 2(9)(A), (C) (defining PII as “information that identifies or is linked or reasonably linkable to a specific individual” (emphasis added)); S. 3300 § 3(5) (defining PII as “any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or device,” including “inferences drawn from any of [this] information . . . to create a profile about an individual reflecting the individual’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes” (emphasis added)).
a list of specific types of information, which can be too restrictive to adequately protect data.\footnote{121} However, because this broader definition employed by lawmakers does not account for PII’s flexible nature and because the boundaries of PII versus non-PII are still unknown, businesses contend that they are burdened with the risk of interpreting PII’s tricky boundaries.\footnote{122} According to Schwartz and Solove, businesses are also asked to endeavor in counterintuitive practices, given that they must build processes to link reasonably linkable information to satisfy individual rights like access, correction, and portability.\footnote{123} And this feat becomes even more difficult and complex when a bill bans this identification process.\footnote{124} Critics also note that this approach is too onerous, posing substantial initial and ongoing compliance costs that could have a disparate impact on businesses.\footnote{125} Under California’s CCPA, for example, nonprofits and businesses with annual revenues under $25 million are exempt from data protection requirements, even though the sensitivity of the data collected and the consequences of compromise are the same.\footnote{126} Meanwhile, one report has already found that companies subject to the requirements may have to pay up to $55 billion in initial compliance costs as a result of the CCPA alone.\footnote{127}

Likewise, a laundry list of unlimited consumer rights may also pose some unintended consequences. Data portability, for example,
could breed anticompetitive outcomes. And more importantly, requirements like right of access and data portability, which require a business to collect all information related to an individual and produce a record of it, risk a new and formidable privacy threat—an individual’s entire data profile could be fraudulently requested and used to harm the individual.

Finally, a significant critique of the consumer control approach is that it places “too much of [a] burden on individual[] [consumers] to manage their [own] privacy.” To exercise control, consumers are tasked with upgrading their digital literacy and monitoring their data for each business interaction, as data collection “becom[es] more sophisticated and less transparent every day.” However, research actually reveals that consumers do not read or understand privacy policies, are heavily influenced by the way choice is framed, and harbor many preexisting and incorrect assumptions about what policies protect. As such, congressional members like New Jersey Representative Frank Pallone (D), Mississippi Senator Roger Wicker (R), and Washington Senator Maria Cantwell (D) have all labeled privacy policies as “unrealistic and unfair,” “lengthy and confusing,” and “no longer enough,” respectively.

---

128. RILA Comment Letter, supra note 68, at 2.
130. Kerry, supra note 71 (noting that though consumer control, namely “[g]reater transparency and individual decision-making,” certainly “[has] a place in comprehensive privacy legislation,” consumer control approaches “are far from sufficient in a digital environment in which control is so elusive” and put “too much of the burden on individuals to manage their privacy protection”).
131. James P. Nehf, The FTC’s Proposed Framework for Privacy Protection Online: A Move Toward Substantive Controls or Just More Notice and Choice?, 37 WM. MITCHELL L. REV. 1727, 1734–43 (2011) (providing several reasons why consumers are not capable of protecting their own privacy); see also Altshuler, supra note 4; Zarsky, supra note 19 (arguing that a majority of consumers are disinterested in managing the particulars of their personal information).
132. See, e.g., Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1883–88 (2013) (describing cognitive and structural problems that consumers have with privacy self-management). According to a recent study, only around “one-in-five adults overall say they always . . . or often . . . read a company’s privacy policy before agreeing to it,” with only 22% of adults who ever read a privacy policy saying they read it all the way. Auxier et al., supra note 19.
133. Kerry & Chin, supra note 116 (first quoting New Jersey Representative Frank Pallone; then quoting Mississippi Senator Roger Wicker; and then quoting Washington Senator Maria Cantwell).
2. Business Accountability Approach

The second approach to privacy reform shifts the responsibility of protecting privacy from consumers to the businesses that hold their data.134 Rather than focusing on consumer ownership of data, this second approach focuses on business conduct and what happens to the data once it is collected.135

Because “overly prescriptive [models] can result in compliance checklists that stymie innovative privacy solutions,” some of these types of proposals offer more flexible behavioral standards.136 These standards allow for flexibility in developing solutions based on a business’s particular circumstances, in contrast to strict, one-size-fits-all rules.137 For example, Intel proposed legislation that includes a general duty of care “to take reasonable . . . measures not to intentionally process personal data in a manner that would have the reasonably foreseeable consequence of directly causing a natural person to suffer significant physical injury or unmerited . . . financial loss.”138

Moreover, although consumers may still be given various rights to their data under this approach, these rights are generally limited when they become unduly burdensome or create impracticability for businesses.139 For example, the Center for Democracy and Technology put forth draft privacy legislation that allows for the right

134. See Kerry, supra note 71; SENATE DEMOCRATS, supra note 70, at 2 (calling for “real accountability” by shifting “the responsibility and liability of protecting privacy from consumers, who are overly burdened with understanding complicated, take-it-or-leave-it privacy policies, to the entities that hold their data and their senior corporate executives”).

135. See Kerry, supra note 71.

136. See Developing the Administration’s Approach to Consumer Privacy, 83 Fed. Reg. 48,600, 48,600–01 (Sept. 26, 2018) (differentiating between strict, principle-based approaches, like models that mandate notice and choice, and those that focus on organizational practices without dictating what the practices should be).

137. See id.

138. Intel Legislation, supra note 70; see also Kerry, supra note 71 (analyzing the implications of this duty of care).

139. See CDT FEDERAL BASELINE, supra note 70, at 2–4 (providing a right of data portability only “[w]here technically feasible”; a right of deletion, along with a list of exceptions, such as if fulfillment would create a legitimate risk to privacy; and a right of correction within limited situations); Intel Legislation, supra note 70 (proposing consumers have “reasonable access to . . . personal data” and “reasonable obscurity of personal data” where it “is likely to create significant privacy risk to the individual that is disproportionate to the public benefit”).
of correction but limits this right to situations where the data is health information, or it could be used for an eligibility determination or educational opportunity.140

Another hallmark of this approach is the use of accountability mechanisms that place the burden of ensuring compliance on the businesses and senior executives who hold consumer data, rather than on the consumer.141 For example, one bill provides for businesses to designate a privacy officer, a data security officer, and internal controls to ensure that senior management is involved in risk assessment.142 The FTC’s routine practice of investigating and charging individual executives of small firms for privacy violations to motivate other executives to ensure compliance is also illustrative of this point.143 Accordingly, rather than advocating for private rights of action, this second approach proposes stronger enforcement, navigated through more capable backstops like state attorneys general, in addition to a federal privacy enforcer.144

In defining PII, these models largely replicate definitions existing in consumer control models, but they appear to make greater allowances for uses of aggregated data.145 However, unlike many consumer control bills and proposals, this second approach places emphasis on transparency and makes some departure from notions of consent, with one proposal by the Center for Democracy and Technology specifically outlining unfair data process practices.146

140. CDT FEDERAL BASELINE, supra note 70, at 2–3.
141. See USCDPA, supra note 69, at 19. See generally CDT FEDERAL BASELINE, supra note 70 (providing obligations of covered entities regarding personal information and outlining prohibited categories of data use except as necessary to deliver specific features or services).
142. See USCDPA, supra note 69, at 19.
143. Dissenting Statement of Commissioner Chopra, supra note 3, at 11, 19 (finding that there is precedent for the FTC to charge individual officers and hold them personally liable and dissenting on the release of CEO Mark Zuckerberg and other executives, counseling that, like executives at small companies who are “routinely” charged, they should be held accountable); Dissenting Statement of Commissioner Slaughter, supra note 3, at 6, 14.
144. USCDPA, supra note 69, at 20–22.
145. Compare USCDPA, supra note 69, at 2–3 (excluding aggregated, de-identified data from the definition of covered data), with S. 3300, 116th Cong. § 3(5) (2020) (including “inferences drawn” from any linked or reasonably linkable information “to create a profile about an individual reflecting the individual’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes” within the definition of covered data).
146. CDT FEDERAL BASELINE, supra note 70, at 10–12.
Notably, business accountability models were less popular than consumer control models in the 116th Congress. But experts attribute this adoption rate to difficulties in formalizing standards and the obvious political appeal of models that appear to give consumers full control.\textsuperscript{147} Elements of business behavior are also beginning to appear in consumer control models.\textsuperscript{148} Nonetheless, as digitalization of information magnifies the harm to individual privacy, critics demand that corporate titans, concerned only with their bottom lines, must be checked.\textsuperscript{149}

III. PROPOSAL

Discussions surrounding information privacy reform boil down to two key competing interests: the need to secure consumers’ personal information and the need to preserve technological innovation and business competitiveness.\textsuperscript{150} Long-running, irreconcilable differences have shown that no solution will elegantly resolve these competing interests.\textsuperscript{151} Additionally, the ever-expanding universe of issues dealing with information privacy and the remarkable diversity among the industries and businesses being regulated give hope for a one-size-fits-all band-aid even less promising.\textsuperscript{152}

As such, focusing first on smaller federal acts targeting some of the bigger gaps and outliers, like brick-and-mortar analytics technologies, could be one way to finally gain some traction.\textsuperscript{153} Recent events, including a string of data breaches, the passage of strict privacy laws in Europe and California, and pressure from

\textsuperscript{147} See Bambauer Statement, supra note 110, at 6.
\textsuperscript{148} Kerry, supra note 71.
\textsuperscript{149} See generally Press Release, supra note 111.
\textsuperscript{150} Altshuler, supra note 4.
\textsuperscript{151} See sources cited supra note 13; David McCabe, Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html [https://perma.cc/L52M-SVD2] (noting that back in 2019 in a “rare” moment, Republicans and Democrats in Congress were all in agreement that a national privacy law is warranted, but “a national privacy law is nowhere in sight”).
\textsuperscript{152} See Kerry, supra note 13.
consumers, have renewed interest in a federal privacy law and may have created the perfect incubator for its passage.  

A. A Uniform Privacy Landscape

Under current U.S. information privacy protections, neither consumers nor businesses are afforded any assurances in navigating today’s challenging and evolving privacy landscape. In response to delayed federal action, state governments are moving to pick up the privacy torch. Without some uniformity, however, movement on information privacy reform could crush companies doing business in more than one state and subject them to the effects of disparate and incomprehensible laws that could change each year. The price tag on California’s new privacy law has already been estimated at $55 billion, and price tags like this across the United States could wreak havoc for businesses and risk the United States ceding its position as a technology leader.

High compliance costs from state laws would also impact businesses disparately. Instead of disrupting the concerning data practices of corporate giants like Facebook and Google, these burdens could actually be most detrimental for smaller businesses.


155. See Beckerman, supra note 57; Kerry & Chin, supra note 116.

156. Serrato et al., supra note 42. As of March 2018, all fifty U.S. states, as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands, have already enacted legislation to expand data breach notification rules, including an expanded definition of personal information, to mirror some of the protections the GDPR provides. Id.; Security Breach Notification Laws, NAT’L CONF. OF STATE LEGISLATURES (July 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/77FB-HUNC].

157. Beckerman, supra note 57; see also Bambauer Statement, supra note 110, at 2 (explaining the significant effects on the economy likely to occur with the passage of just the CCPA). See generally Campbell et al., supra note 125.

158. Bambauer Statement, supra note 110, at 2 (asserting that “after a painful transition phase, the [CCPA] will cause long-term drag on innovation,” which should provide reason for pause given that “[t]he tech sector is the crown jewel of the U.S. economy”—it is “the greatest source of productivity growth, [and] it also produces jobs and raises wages faster than any other industry”); Feiner, supra note 127; NRF Comment Letter, supra note 67; Beckerman, supra note 57.

159. See generally Ivana Kottasová, These Companies Are Getting Killed by GDPR, CNN: BUSINESS
In practice, these costs could force smaller businesses to close shop, wiping out the competition for and further concentrating personal information in the hands of the big players.160 “And even after a painful transition phase, [these laws] will cause long-term drag on innovation.”161

This result is particularly irreconcilable given that the very consumers these laws serve to protect would also be victims of this patchwork of state laws. Because data protection would necessarily depend on the criteria chosen by the states to trigger compliance, personal data still would not be protected comprehensively.162 Thus, consumers would be given a false sense of security concerning the strength of privacy protections and encounter little legal certainty or predictability.163

Additionally, consumers could also face increased costs as businesses shift these expenses onto their products and services. And because businesses might be less inclined to act in certain areas for fear of risking penalties, consumers would likely forfeit many of the conveniences and benefits they have come to expect thanks to innovative uses of data.164 As such, a uniform privacy landscape appears most beneficial for both consumers and businesses.165

Although advocates fear that preempting state laws will dilute stronger consumer protections, preemption would apply only to inconsistent state laws confined to the limited context of

---

160. Bambauer Statement, supra note 110, at 2. See generally Kottasová, supra note 159; Campbell et al., supra note 125; Feiner, supra note 127.


162. See, e.g., CAL. CIV. CODE § 1798.140 (West 2020) (denying protections to the data of nonprofits and businesses if those organizations have annual revenues under $25 million dollars or meet other similar criteria).

163. Beckerman, supra note 57. According to a Pew Research study, there is already a “general lack of understanding about data privacy laws” among consumers, with 63% stating that “they understand very little or nothing at all about the laws and regulations that are currently in place to protect their data privacy.” Auxier et al., supra note 19.

164. NRF Comment Letter, supra note 67.

165. See generally Beckerman, supra note 57.
brick-and-mortar. Further, a federal law could actually provide stronger, more comprehensive protections that eliminate gaps in state laws and issues with patchwork compliance.  

B. A Targeted Brick-and-Mortar Technology Privacy Act

Concern for brick-and-mortar is well-founded given retail’s importance to the U.S. economy with a gross domestic product contribution of around $3.9 trillion of the annual total of $21.43 trillion. Despite all of the attention legislators and academics continue to give online privacy, online retail transactions constitute around only 11% of all U.S. retail sales—with brick-and-mortar controlling the rest, totaling approximately $3.38 trillion. Further, although online and brick-and-mortar retailers both seek to improve and personalize the shopping experience through analytics technologies, in practice information privacy laws that treat them the same could create very different outcomes for each.

Ambiguity and a hodgepodge of sweeping state information privacy laws have the propensity to suffocate the use of technologies

166. See, e.g., Cameron F. Kerry, A Federal Privacy Law Could Do Better Than California’s, BROOKINGS: TECHTANK (Apr. 29, 2019), https://www.brookings.edu/blog/techtank/2019/04/29/a-federal-privacy-law-could-do-better-than-californias/ [https://perma.cc/P3C8-36K5] (noting how privacy advocates and California representatives in Congress feel the CCPA must be insulated from preemption); Privacy Preemption Watch, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/preemption/ [https://perma.cc/L5Q8-P3C8] (advocating for a federal baseline law and arguing that preemption stops states from performing their traditional roles as “laboratories of democracy” (quoting New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932)) (Brandeis, J., dissenting)).  

167. Kerry, supra note 166.  


170. See discussion supra Sections II.A.2, II.B.1.
that often take years to develop and roll out across physical retail locations. Legacy infrastructures and the realities of operating at scale in a three-dimensional space require significant planning, engineering, manpower, and outlays of capital that could easily favor online over brick-and-mortar retail. As such, neither the bills and drafts introduced in the 116th Congress nor GDPR-, CCPA-, or CPRA-style laws adequately provide a clear path for developing and implementing in-store technology. Moreover, unlike the wealth of FTC settlements, likened to common law and available for online privacy, counsel in the brick-and-mortar context is noticeably absent and several questions remain unanswered. This is particularly problematic given that the risks and costs of innovation are significantly higher in brick-and-mortar than online—a miscalculation cannot be remedied with keystrokes and lines of code.

Additionally, because in-store analytics technologies are just beginning to gain traction, a targeted federal act will allow policymakers to get in front of information privacy issues. With some healthy guardrails, privacy regulation can grow alongside innovation. And a targeted federal act could serve as a testing and learning ground for privacy policy innovation for possible application across a myriad of other smart spaces on the horizon, such as smart cities, hotels, and factories. Further, rather than working with hundreds of different stakeholders across sectors on each move, policymakers would be able to narrow their focus to the retail sector, allowing for greater efficiency and a better chance of success.

171. See discussion supra Section II.A.2; see also NISSENBAUM, supra note 4, at 27–29 (showing the large differences between technological capabilities online and the three-dimensional store); NRF Comment Letter, supra note 67, at 5–6 (explaining that without some harmonization of regulatory laws, businesses may cease “their investment in technological innovations that would better serve consumers . . . out of fear of tripping over a hodge-podge of potentially conflicting . . . regulations”).
172. See discussion supra Section II.A.2; NISSENBAUM, supra note 4, at 29.
173. See discussion supra Sections II.A.2, II.B.1.
174. See discussion supra Section I.B.
175. See discussion supra Section II.A.2; NISSENBAUM, supra note 4, at 29.
176. See SKORUPA, supra note 26 and accompanying text.
177. Ganesan et al., supra note 6.
Findings from this act could then inform information privacy reform in other relevant sectors.

Although a targeted act lends to a continuation of the sectoral approach generally disfavored by privacy advocates, it may be the best solution to address brick-and-mortar concerns because of its ability to take stock of contextual and informational norms relevant to the industry. This flexibility would allow for more transparent and comprehensive regulation, as it has already done for sectors like healthcare and finance.\textsuperscript{178} And it does not preclude an omnibus law later; a savings provision could simply preserve the act.

C. More Business Accountability and FTC Enforcement

To operate effectively, however, strong accountability and enforcement mechanisms will need to accompany any act. The current privacy regime is generally viewed as insufficient in this regard, yet with popular consumer control models, lawmakers appear to provide consumers with more of the same—“a horse in a self-driving car world.”\textsuperscript{179} At first blush, consumer control models appear to provide consumers with the greatest protections.\textsuperscript{180} In practice, however, they may do just the opposite because they continue to rely on broken consent models and place the responsibility of protecting privacy on consumers, despite recognizing that they are unfit for the task.\textsuperscript{181}

Moreover, simply mirroring a hastily passed CCPA at the expense of businesses will not provide consumers or businesses with a fair or adequate solution.\textsuperscript{182} To properly balance competing consumer and business interests, a federal privacy law should adopt more of a business accountability approach, shifting the burden of protecting privacy to the businesses, data brokers, and executives that hold

\begin{footnotesize}

178. NISSENBAUM, supra note 4, at 238.
180. See discussion supra Section II.B.1; see also Bambauer Statement, supra note 110, at 6.
181. See discussion supra Section II.B.1; Bambauer Statement, supra note 110, at 5–6.
182. See Wakabayashi, supra note 58 and accompanying text.
\end{footnotesize}
consumer data, while using duties of care to allow flexibility and innovation to develop systems and processes that do not depend on intrusive surveillance.\footnote{183}{Kerry, supra note 166 ("The effectiveness of [exclusive focus on control] is becoming a mirage as the amount and pace of data collection keeps expanding. . . . Privacy experts widely believe that the law needs to shift the burden away from individuals and onto the businesses that collect personal information.").}

To complement this shift, a federal regulator is also necessary to ensure that profit motives do not lead to blatant violations, like those by Facebook.\footnote{184}{See generally Hoofnagle et al., supra note 49.} Despite concerns that the FTC is not up to the task, no enforcement candidate seems better suited for the job.\footnote{185}{Id.; see also Rich, supra note 49.} The reality is that the FTC’s legal authority over privacy is the same as it was before the internet.\footnote{186}{See Rich, supra note 49 (noting that the FTC Act “was passed more than 100 years ago, long before personal computers, the internet, social media or mobile phones were invented” and is no longer enough to protect privacy).} The FTC also remains “woefully understaffed in privacy, with some [forty] full-time staff members . . . dedicated to protecting the privacy of more than 320 million Americans” and overseeing over 32 million businesses.\footnote{187}{Id.; Todd Kehoe, What Counts As a ‘Business’? It Might Not Be What You Think It Is, ALBANY BUS. REV.: DATA DROP (Apr. 11, 2019, 2:39 PM), https://www.bizjournals.com/albany/news/2019/04/11/number-of-businesses-in-the-united-states.html [https://perma.cc/AZ9F-Y6H8].} In comparison, Britain has more than 700 staff members, and Ireland and Canada each have almost 150 staff members, despite the fact that both of these countries have smaller populations than the United States.\footnote{188}{Hoofnagle et al., supra note 49; Rich, supra note 49.}

Yet, in spite of these constraints and limited resources, the FTC has earned itself the title of “de facto federal data protection authority,” and unlike any new agency, the FTC has decades of experience in handling privacy issues and appears willing to pursue the corporate giants.\footnote{189}{Solove & Hartzog, supra note 11, at 600; Hoofnagle et al., supra note 49 (noting that even with its severe limitations, the FTC has bolstered important norms, influenced company practices, and become a significant enforcement agency that the industry pays attention to); Rich, supra note 49 (“The F.T.C. has nevertheless built a strong privacy program . . . .”).} As such, the FTC could take on many more cases and step up to lead the U.S. privacy regulatory effort if properly
equipped to do so. Specifically, the FTC should be given greater resources and a staff more proportional to the population size it serves; enhanced enforcement authority, including the ability to impose civil fines for first-time violations; and limited power to interpret specific provisions by adopting rules. Although granting the FTC rulemaking authority has been criticized on account of alleged overreach in the past, the grant here would be limited, thus curtailing any such risk.

Despite this expansion of FTC powers, accountability among corporate titans will still demand more to ensure that the FTC is not simply chasing headlines with drop-in-the-bucket fines, as FTC Commissioner Rohit Chopra has already accused his fellow FTC commissioners of doing. To that end, some bills have sought to empower individuals with a PRA. However, although deputizing individuals as "private attorneys general" would certainly serve as an enforcement multiplier, this measure would again place the burden of enforcing privacy on consumers who would either be excluded by or forced to absorb the costs of litigation. Notably, a PRA could also bring a reform effort to an impasse.

190. See generally Hoofnagle et al., supra note 49.
191. See generally Rich, supra note 49.
192. Propes, supra note 73.
194. See Press Release, supra note 111; Kerry, supra note 71; Bambauer Statement, supra note 110, at 3 and accompanying text.
195. Birnbaum, supra note 40 (noting that a PRA is one of two issues that has stalled negotiations for months and pointing out that the House’s latest bipartisan federal draft bill has sidestepped the PRA issue to try to move forward). See generally Theodore F. Claypoole, Private Right of Action vs. Statutory Damages. Which Has More Impact?, NAT’L. L. REV. (Aug. 2, 2019), https://www.natlawreview.com/article/private-right-action-vs-statutory-damages—which-has-more-impact [https://perma.cc/R4BL-HBDL] (offering insight into one side of the PRA debate focused on concerns for nuisance lawsuits and class-actions, arguing that a PRA could lead to a slew of frivolous, resource-consuming lawsuits). But see generally Joseph Jerome, Private Right of Action Shouldn’t Be a Yes-No Proposition in Federal US Privacy Legislation, IAPP (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/ [https://perma.cc/6APU-WVGU] (explaining that Congress and the courts have a huge say in how much litigation results, noting the benefits of a PRA, and arguing that if properly constructed, a PRA could advance privacy rights at the national level); Cameron F. Kerry & John B. Morris, In Privacy Legislation, a Private Right of Action Is Not an All-or-Nothing Proposition, BROOKINGS:
Instead, consumers might be better served by providing accountability and personal liability for corporate executives, empowering and appropriately staffing the FTC, and using state attorneys general as an enforcement backstop. Under the Children’s Online Privacy Protection Act (COPPA), the FTC and state attorneys general have already proven that they can successfully share enforcement powers. Enforcement through these capable means would also provide consumers with consistent outcomes and provide a more robust process through which noncompliance could be steadily monitored and remedied.

D. Specific Brick-and-Mortar Considerations

One-size-fits-all approaches provided in industry-neutral and channel-neutral provisions are unrealistic and “untethered to the realities of operating at scale” in the physical retail environment. Instead, a uniform act could provide much-needed clarity for both the brick-and-mortar store and the consumer. Specific considerations should include: a fixed, narrow definition of PII; reasonable consumer control; a general duty of care; and enhanced notice via modern technology solutions.

1. Fixed, Narrow Definition of PII

PII is probably best described as a moving target; distinctions between PII and non-PII are not fixed and depend upon ever-changing technological capabilities to reidentify non-PII such that “today’s non-PII might be tomorrow’s PII.” Because of this malleable nature, broad definitions such as “linked or reasonably...
linkable” are unclear and unfairly place all of the risk on brick-and-mortar businesses. Instead, a fixed, narrow definition of PII should be used to trigger the greatest business obligations based on truly sensitive, individually identifiable information linked to a real risk of significant harm.201

As such, aggregated and de-identified information, for which a company has no reasonable basis to believe could be used to identify an individual, should be expressly excluded from this definition. A de-identification standard, which outlines permitted methods for achieving de-identification, could be used to prevent users from circumventing compliance.202 Further, as an additional consideration, PII could be classified regarding the specific context of brick-and-mortar data processing, rather than regarding generic determinations, which may not address relevant categories of information.203

Although broader definitions of PII may better address technological advances, a catch-all, like “any other identifier that the FTC determines as identifiable,” could be added to the definition to account for this needed flexibility.204 Even with this addition, this fixed definition would create a clearer understanding of business obligations and consumer rights. It would also reduce compliance expenses stemming from broad definitions of PII and allow businesses the flexibility to continue innovating and serving consumers in expected and convenient ways.

201. See RILA Comment Letter, supra note 68, at 2.
202. See, e.g., U.S. DEP’T OF HEALTH & HUM. SERVS., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE 6–9 (2015). Under HIPAA, there are two methods to achieve de-identification: (1) through expert determination and (2) through removal of a list of specified identifiers coupled with no actual knowledge that the information could be used to identify an individual who is a subject of the information. Id. at 7.
203. See Schwartz & Solove, supra note 36, at 1847–48 (explaining that abstract determinations of PII are insufficient because the ability to identify information is driven by context, and providing explanatory examples); see also RILA Comment Letter, supra note 68, at 2 (making a similar argument).
204. See, e.g., 15 U.S.C. § 6501(8)(F) (“The term ‘personal information’ means individually identifiable information about an individual collected online, including . . . any other identifier that the Commission determines permits the physical or online contacting of a specific individual . . . ”). Under this authority, the FTC has indeed acted to expand the definition of PII in COPPA. Schwartz & Solove, supra note 36, at 1835.
2. General Duty of Care

Additionally, including a general duty of care—like some of the 116th Congress drafts—could provide a second tier of protections for data that falls outside the definition of PII. This duty of care could include reasonable measures not to cause reasonably foreseeable harm during data collection and use; not to discriminate based on things like religion, sexual orientation, income, medical conditions, or political beliefs; to collect and retain only the minimum data necessary to carry out purposes reasonably expected in the relationship; and to use security practices proportional to the sensitivity of data. For example, a brick-and-mortar store capturing location data through mobile analytics should never be capturing full location trails extending outside the store, including details such as other places visited with timestamps, to construct a consumer’s daily journey. Even if this information was not captured within the definition of PII, this intrusive overreach would easily be captured under this duty of care.

With respect to in-store analytics technologies, rather than arbitrarily excluding uncommon technologies, this narrow definition of PII and general duty of care properly allow for consideration of technology use in context. Brick-and-mortar stores are not prohibited from using less invasive technologies to gather invaluable survival metrics while still appreciating the consumer’s need for privacy. Anonymized video analytics, for example, which scan video frames to detect the presence of a face—but do not recognize a face individually and destroy the video after detection—offer a positive-sum, “win-win” solution that stores could use to capture

205. See Intel Legislation, supra note 70; Kerry, supra note 71.
207. See NISSENBAUM, supra note 4, at 235. Helen Nissenbaum cautioned against applying moral categories to technologies without considering context. See id. (“What matters is not merely that a particular technical device or system is not overly unusual, but that its use in a particular context, in a particular way is not overly unusual.” (emphasis omitted)); see also Bambauer Statement, supra note 110, at 4 (arguing against user control models because of the potential for “overprotection when consumers distrust a new data practice that is actually socially and even personally beneficial”).
many of the metrics discussed in Part I in a privacy-enhancing way.  

3. Reasonable Consumer Control

To further balance business practicality and burdens, a “reasonableness” limitation could also be placed on offered consumer rights. Despite political demand, GDPR- and CCPA-style models that attempt to give consumers full control of PII often paint an illusory picture for consumers or fail to actually serve consumer privacy interests. These models position privacy as something consumers can protect themselves against, but—even with best practices—the reality of engaging with most technology and participating in the digital economy means handing over data. Consumers can also quickly become inundated by obvious or seemingly insignificant choices and become less attentive to choices that are important to them.


209. Bambauer Statement, supra note 110, at 6; Kerry, supra note 71 (noting that although consumer control, namely greater transparency and individual decision-making, “has a place in comprehensive privacy legislation,” consumer control approaches “are far from sufficient in a digital environment in which control is so elusive”).


Full consumer control also presents a risk of burdening the digital economy with heavy transaction costs, despite little reason to think that compliance will have a meaningful relationship to mitigating consumer harms. Data portability provisions are illustrative of this point. Arming consumers with the option to move their data from one business to another does little to further privacy protection goals. Individual control is not the same as individual privacy. Moreover, it creates a substantial and unnecessary privacy risk.

As such, because data collection practices vary widely from one business to the next, decisions regarding which consumer rights to offer, when to offer them, and how they are offered should also depend on context. A privacy approach that evaluates these rights in context better addresses the unique needs and uses of data by brick-and-mortar stores. Specifically concerning consent, to avoid consent fatigue, a more proportional risk-based concept of consent that requires explicit consent only where serious harm is threatened could offer a more practical solution in the context of the store environment and help make consumer choice more meaningful.


Based on the bills and proposals before the 116th Congress, it is clear that notice or awareness continues to be a key concern. However, lengthy and legalistic privacy policies are wholly ineffective in actually informing consumers of data practices, even if they do serve an accountability function for privacy watchdogs.

214. See PAVUR & KNERR, supra note 129.
215. Cate, supra note 213, at 1799 (recommending this kind of approach to reduce prohibitive restrictions on health research); see also Kerry, supra note 13 (noting that perhaps informed consent was practical two decades ago, but in a world with constant streams of digital interactions, today it “is a fantasy”).
216. See PAVUR & KNERR, supra note 129.
217. Kerry, supra note 71; see also Joseph Turow, Opinion, Let’s Retire the Phrase ‘Privacy Policy,’ N.Y. TIMES (Aug. 20, 2018), https://www.nytimes.com/2018/08/20/opinion/20Turow.html [https://perma.cc/JN4B-WCMP] (noting that a majority of consumers actually interpret the mere presence of a privacy policy on a business’s website as an indication that it will not share the individual’s information with other websites or companies without the consumer’s permission).
Additionally, in the specific context of in-store analytics technologies, notices placed on websites or signs placed at store entrances can be problematic given that these technologies are largely invisible to consumers inside the store.218

As an immediate solution for stores that also have an online presence, as regulators have done with the GDPR, a privacy policy template could be created to at least standardize how and what information is presented across websites.219 Additionally, because notice must serve the purpose of both informing consumers and acting as an accountability mechanism, creating a two-tiered system appears to offer a simple solution here.220 For regulators, a plain disclosure on data practices for consumers and periodic data protection reports certified by business executives could be required.221 For consumers, a short and simple notice on the business’s website with options to dive deeper and get more details on data practices could be required.222 Disclosures based on the information disclosed in executive certifications could also be communicated via a centralized consumer website using standardized icons, short explanatory videos, and privacy practice scores, much like restaurant health inspection scores.

At the store level, in addition to a notice placed outside the store, businesses could also place notices at the shelf-level or at other relevant points within the store to drive further awareness. And, looking to the future, many of the same technologies used for tracking consumers could also be used to provide solutions to improve transparency. In one scenario, these devices could be

---

220. Kerry & Chin, supra note 116 (detailing the benefits and workings of a two-tiered approach).
221. Id.
required to “announce” the technology’s presence to consumers by broadcasting a standardized, continuous wireless signal when in use, which could be presented to consumers in a myriad of ways.\textsuperscript{223} For example, in dealing with video analytics, a standardized mobile application could sniff out these technologies and provide the consumer with a live view into shopper tracking technologies used within the store.\textsuperscript{224}

In dealing with mobile tracking solutions, open Wi-Fi or Bluetooth networks could also push a mobile alert to users of the existence of mobile tracking and allow these consumers to opt out.\textsuperscript{225} Alternatively, a standardized privacy-enhancing app could allow users to automatically disable signal transmission when approaching these networks to avoid collection altogether.\textsuperscript{226} In another scenario, a consumer’s data collection and use preferences could be programmed into the consumer’s smartphone or wearable device, like a smartwatch, and used to communicate their privacy preferences to the tracking devices.\textsuperscript{227}

Although a technology-driven solution certainly presents several implementation challenges, the reality is that the complexity of today’s technological landscape and the widespread consumer adoption of smartphones and other technologies suggest that these ideas have come of age for advancing privacy outcomes.\textsuperscript{228} The communication norms of modern consumers are very different than the norms of consumers targeted by the 1980 FIPs and even the norms of consumers considered by the 116th Congress’s bills and resolutions.\textsuperscript{229} The question is, thus, whether Congress will delay the

\textsuperscript{223} Soltani, supra note 9 (suggesting that passive technology devices could automatically broadcast standardized, semicontinuous wireless signals that announce their presence as a technical solution to pervasive data collection in the public sphere).


\textsuperscript{225} Soltani, supra note 9.

\textsuperscript{226} Id.

\textsuperscript{227} WORLD ECON. F., supra note 218, at 22–23.

\textsuperscript{228} Id. at 24.

\textsuperscript{229} See Nehf, supra note 131, at 1733.
inevitable and make a difficult, eleventh-hour decision after industries and businesses are already established, or whether Congress will act now while brick-and-mortar technologies are still in the early phases of adoption and implementation, which would arguably be easier. Failures in reaching consumers with notice-and-consent solutions have at least proven that moving forward, a new approach is necessary. If the problem is technology, perhaps technology could also offer the solution?

CONCLUSION

Large gaps in current information privacy regulation have left consumers and businesses alike unsure of the extent of privacy protections afforded. One sector of particular concern is the approximately $3.38 trillion brick-and-mortar retail industry and specifically its growing adoption of in-store analytics technologies. Despite renewed interest in privacy reform, these efforts have focused largely on online information privacy, leaving many questions as to the fate of new and emerging brick-and-mortar technologies that mimic online tracking. Because these in-store analytics technologies are critical to helping traditional stores regain relevance among modern shoppers and compete against online competitors, there is a dire need to create a focused information privacy act. Otherwise, in-store analytics technologies could be swept up under broader online privacy reform and rendered obsolete. A targeted, uniform federal privacy act will ensure that consumers do not pay with their privacy and that brick-and-mortar stores secure a place in the future.

230. See id.; SENATE DEMOCRATS, supra note 70; Kerry, supra note 71; Developing the Administration’s Approach to Consumer Privacy, 83 Fed. Reg. 48,600, 48,601 (Sept. 26, 2018) (emphasizing that, to date, notice-and-choice mandates have resulted primarily in long, legal, regulator-focused privacy policies, only helping a small number of users).
231. See discussion supra Section II.A.
232. See NRF Forecasts, supra note 169; GDP Q4 2019, supra note 168.
233. See discussion supra Sections II.A.1, II.A.2.
234. See discussion supra Part I.