Georgia State University Law Review

Volume 37
Issue 3 *Spring 2021*

Article 10

8-1-2021

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

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

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]

---

1. Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/CMU4-EVD7]; Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making*, FED. TRADE COMM'N: BUS. BLOG (July 24, 2019, 8:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history [https://perma.cc/Q5DB-RS6D]; Michael Nuñez, *FTC Slaps Facebook with $5 Billion Fine, Forces New Privacy Controls*, FORBES (July 24, 2019, 12:05 PM), https://www.forbes.com/sites/mnunez/2019/07/24/ftcs-unprecedented-slap-fines-facebook-5-billion-forces-new-privacy-controls/#3871ada05668.

2. Press Release, *supra* note 1.

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/1536918/182_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., https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/archive-of-the-meetings-of-the-secretarys-advisory-committee-on-automated-personal-data-systems-sacapds/ [https://perma.cc/6AMM-R2RZ] (reading 1973 transcripts from the committee that

For a long time, information privacy concerns have focused on cyberspace—social media and e-commerce.[5] 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.[6] 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]

---

delivered the principles underlying modern privacy legislation and observing that "it is striking how little conversations about privacy have changed in forty years"); Tehilla Shwartz Altshuler, *Privacy in a Digital World*, TECHCRUNCH (Sept. 26, 2019, 5:00 PM), https://techcrunch.com/2019/09/26/privacy-queen-of-human-rights-in-a-digital-world (explaining how technological progress has caused tension "between the right to privacy and the extensive data pooling on which the digital economy is based"). For a more recent example of this tension, consider the outrage surrounding use of Clearview AI's facial recognition technology to support law enforcement efforts and contact tracing after the COVID-19 pandemic. Jacob Ward & Chiara Sottile, *A Facial Recognition Company Wants to Help with Contact Tracing. A Senator Has Questions.*, NBC NEWS (Apr. 30, 2020, 9:29 PM), https://www.nbcnews.com/tech/security/facial-recognition-company-wants-help-contact-tracing-senator-has-questions-n1197291 [https://perma.cc/TZ8G-5EJH].

5. John D. McKinnon, *Big Brother at the Mall*, WALL ST. J.: BUS. (Apr. 13, 2019, 12:00 AM), https://www.wsj.com/articles/big-brother-in-the-mall-11555128005 [https://perma.cc/LQ3V-SXGX].

6. *Id.*; Altshuler, *supra* note 4; Lisa Terry, *Shopper Tracking: Reinventing and Reimagining the Store Experience*, RIS NEWS (May 31, 2019), https://risnews.com/shopper-tracking-reinventing-and-reimagining-store-experience [https://perma.cc/VS9P-S8ER] ("Innovations in cameras, sensors, RFID, mobile, edge computing and networking technologies are giving retailers new insight . . . ."). *See generally* Ronny Max, *19 Technologies of People Tracking*, BEHAV. ANALYTICS RETAIL (Jan. 27, 2021), https://behavioranalyticsretail.com/technologies-tracking-people/ (explaining how brick-and-mortar technologies are becoming more cost-effective and accurate in real-time); Drew FitzGerald, *5G Race Could Leave Personal Privacy in the Dust*, WALL ST. J.: BUS. (Nov. 11, 2019, 10:00 PM), https://www.wsj.com/articles/5g-race-could-leave-personal-privacy-in-the-dust-11573527600 [https://perma.cc/54PZ-L6TH] ("[N]ew 5G networks are expected to bring billions of cameras, sensors and other 'smart' devices . . . . [online, all collecting] reams of data from the world around them . . . ."). Retail is not the only industry affected by technology growth and adoption—smart cities, smart vehicles, and smart factories are all in the works. Vasanth Ganesan et al., *Video Meets the Internet of Things*, MCKINSEY & CO. (Dec. 7, 2016), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/video-meets-the-internet-of-things [https://perma.cc/5SWD-X6T8]; *see also* Melissa Locker, *Facial Recognition Is Coming to Hotels to Make Check-In Easier—and Much Creepier*, FAST CO. (Apr. 1, 2019), https://www.fastcompany.com/90327875/facial-recognition-is-coming-to-hotels-to-make-check-in-easier-and-much-creepier (describing an ultra-modern boutique hotel in China that lets guests "scan their faces to expedite the [check-in] process"; make requests through an "Alexa-like assistant" that controls the temperature, curtains, and lights; and receive room service deliveries and bar drinks via robots).

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.[8] However, the premise of in-store tracking has left some consumer advocates, academics, and key committee leaders in both the House and Senate uneasy.[9] This uneasiness is further underscored by the fact that these tracking technologies are often invisible to the average shopper.[10] 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.[11] 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.[12]

---

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*], http://www.videomining.com/newsroom/articles-white-papers/videomining-frequently-asked-questions [https://perma.cc/HQ9K-M7L4]; *see also* Max, *supra* note 6. In contrast, mobile analytics, such as Wi-Fi analytics, listens for signals from the shopper's mobile device to detect presence in-store and captures location data, among other metrics, to optimize in-store performance. WALKBASE, WI-FI ANALYTICS FOR RETAIL STORES: BUYER'S GUIDE 11 (2016), https://s3.amazonaws.com/wlkbase/Whitepapers/whitepaper-walkbase-wifi-analytics-buyers-guide.pdf [https://perma.cc/GQ3D-SC99].

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").

9. McKinnon, *supra* note 5; *see also* Daniel Keyes, *New In-Store Technologies Could Bring About Stricter Regulations*, BUS. INSIDER: RETAIL (Apr. 16, 2019, 10:25 AM), https://www.businessinsider.com/new-in-store-technologies-may-bring-regulations-2019-4 [https://perma.cc/69ET-ZTYT]; Ashkan Soltani, *Privacy Trade-Offs in Retail Tracking*, FED. TRADE COMM'N: TECH@FTC (Apr. 30, 2015, 11:59 AM), https://www.ftc.gov/news-events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking [https://perma.cc/WP5N-FCAE] (describing the "obscure" and "controversial" nature of retail tracking and noting consumer distrust with the technology).

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 Porta-Potty Can Teach Designers About Digital Privacy*, FAST CO. (Sept. 27, 2019), https://www.fastcompany.com/90409598/what-the-first-porta-potty-can-teach-designers-about-digital-privacy [https://perma.cc/K7QS-X5H2] ("Without sights, sounds, and touch, [data privacy] feels practically invisible.").

11. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

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.[13] 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.[14] 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.[15]

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)).

13. Allison Grande, *What to Watch As Congress Mulls Federal Privacy Legislation*, LAW360 (Feb. 25, 2019, 9:44 PM), https://www.law360.com/articles/1132337/what-to-watch-as-congress-mulls-federal-privacy-legislation; *see also* Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ (inferring that multinational corporations and business interests have long posed a roadblock to uniform privacy law development, given little incentive and a daunting outlook on dealing with comprehensive law); Natasha Singer, *Why a Push for Online Privacy Is Bogged Down in Washington*, N.Y. TIMES (Feb. 28, 2016), https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html [https://perma.cc/4MVB-T3KH] (providing an illustrative example of how online privacy initiatives have been subject to "gridlock" due to "clashing visions for American society and commerce" and noting that it "provides an instructive preview of looming battles . . . to come").

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 AISLES 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.[16] 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.[17] 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.[18] 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* McKinnon, *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.").

17. Altshuler, *supra* note 4; Bruce Schneier, *Fear and Convenience*, *in* PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS 200, 202 (Marc Rotenberg et al. eds., 2015) ("Ephemeral conversation is becoming increasingly rare . . . ."). *See generally* Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018, 12:42 AM), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#1baf020260ba [https://perma.cc/7CWE-EWZL] (providing several statistics on the volume and categories of consumer data collected each day); Dylan Curran, Opinion, *Are You Ready? Here Is All the Data Facebook and Google Have on You*, THE GUARDIAN (Mar. 30, 2018, 3:17 AM), https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy [https://perma.cc/94Z3-7BUC] (illustrating the level of personal information companies like Google and Facebook collect on users).

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.[19] 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.[20] As a result, industry experts estimate that this digital economy is "doubling the volume of . . . information in the world every two years."[21]

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.[22]

Release, Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016 (Feb. 7, 2017), https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 [https://perma.cc/W63K-6RUK] (forecasting that approximately 12.8 billion consumer-connected devices would be in use in 2020, more than doubling the estimated 5.2 billion devices in use three years prior).

19. *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/ [https://perma.cc/EJC7-FQJK] ("[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).

20. *See* Angus Hervey, *Privacy Shouldn't Be the Price of Progress. Here's How to Keep Your Data Safe*, QUARTZ (Jan. 26, 2018), https://qz.com/1188898/privacy-shouldnt-be-the-price-of-progress-heres-how-to-keep-your-data-safe/ [https://perma.cc/BV4Z-JK5M]; *see also* Press Release, *supra* note 18; Schneier, *supra* note 17, at 201–02. *See generally* Jonas, *supra* note 18.

21. Kerry, *supra* note 13.

22. ROD SIDES & BRYAN FURMAN, DELOITTE, 2019 RETAIL OUTLOOK: TRANSITION AHEAD 4 (2019), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-cb-retail-outlook-transition-ahead-2019.pdf [https://perma.cc/H8FN-ZH5L]; Hugo Moreno, *How Retailers Can Make the Most of Their Data*, FORBES (June 28, 2018, 1:03 PM), https://www.forbes.com/sites/forbesinsights/2018/06/28/how-retailers-can-make-the-most-of-their-data/#6b2dd99d453c ("Among the industries that have seen their traditional ways of doing business upended by the rapid advent of the internet . . . , retail is perhaps one of the most affected. . . . [I]t's now increasingly difficult for midsize retailers to remain competitive against the ubiquity and scale of global online marketplaces while margins dwindle and the costs of meeting customer expectations only continue to rise."); Jack Karsten & Darrell M. West, *Technology Adoption Powers Shift in Retail Landscape*, BROOKINGS: TECHTANK (May 10, 2017), https://www.brookings.edu/blog/techtank/2017/05/10/technology-adoption-powers-shift-in-retail-landscape/ [https://perma.cc/W772-ZJAQ] ("To stay competitive with online retailers going forward, traditional retailers must match their pace of innovation."); Corinne Ruff, *Do Retailers Need Innovation*

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

Labs to Stay Alive?, RETAIL DIVE: DEEP DIVE (Apr. 11, 2017), https://www.retaildive.com/news/do-retailers-need-innovation-labs-to-stay-alive/440277/ ("Many retailers today are scrambling to keep pace with emerging technologies and changing consumer behaviors. Everyone is trying to create stores of the future . . . .").

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* RETAILWIRE 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/jiawertz/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.

26. Moreno, *supra* note 22; *see also* JOE SKORUPA, RIS NEWS, 29TH ANNUAL RETAIL TECHNOLOGY STUDY: RETAIL ACCELERATES 16 fig.4 (2019), https://risnews.com/29th-annual-retail-technology-study-retail-accelerates.

render stores obsolete.[27] 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.[28]

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.[29] 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.[30]

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.[31] 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.[32] These metrics can be used to optimize layout and store planning, staffing and merchandising, and marketing and promotions.[33]

---

27. Jonas, *supra* note 18; *see also* SIDES & FURMAN, *supra* note 22; SKORUPA, *supra* note 26; Moreno, *supra* note 22.

28. SKORUPA, *supra* note 26, at 14 fig.2, 18. Some online players are also making plans including in-store tracking technologies—retail behemoth Amazon is planning to open 3,000 cashierless stores built on a mix of tracking and other technologies across the U.S. by 2021. Rani Molla, *Amazon's Cashierless Go Stores Could Be a $4 Billion Business by 2021, New Research Suggests*, VOX (Jan. 4, 2019, 10:33 AM), https://www.vox.com/2019/1/4/18166934/amazon-go-stores-revenue-estimates-cashierless.

29. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&ref=charlesduhigg [https://perma.cc/F2TU-BSGP].

30. TUROW, *supra* note 15, at 3; Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July 14, 2013), https://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html [https://perma.cc/S5LB-RSZ2].

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.[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.[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.[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.[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.[38]

(Jan. 5, 2015), https://streetfightmag.com/2015/01/05/finding-the-roi-in-retail-in-store-analytics/#.Xcb7V-dKgn0 [https://perma.cc/U78K-KVPC].

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.

35. Max, *supra* note 6; Schwartz & Solove, *supra* note 34, at 879.

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.

37. NISSENBAUM, *supra* note 4, at 43; SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 8 (2019); Altshuler, *supra* note 4.

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.[39] Likewise, minorities and other groups could also receive disparate treatment based on data collected.[40] 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.[41]

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.[42] However, as it stands, the Constitution does not explicitly

---

profile (quoting Danielle Citron, law professor at University of Maryland School of Law)).

39. TUROW, *supra* note 15, at 10–11.

40. *See* Emily Birnbaum, *Key House Committee Offers Online Privacy Bill Draft*, THE HILL (Dec. 18, 2019, 5:16 PM), https://thehill.com/policy/technology/475191-key-house-committee-offers-online-privacy-bill-draft [https://perma.cc/ZX5P-3X7B] (noting that the first draft of a bipartisan federal privacy bill includes specific provisions "bar[ring] companies from using data in ways that result in discrimination against minorities and other populations").

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.[43] Instead, privacy laws are largely a sectoral hodgepodge of differing governmental views on consumers' rights, leaving several unregulated gaps.[44] 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.[45] 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.[46]

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

40 (highlighting bipartisan support for a federal privacy bill). *See generally* Jeewon Kim Serrato et al., *U.S. States Pass Data Protection Laws on the Heels of the GDPR*, NORTON ROSE FULBRIGHT: DATA PROT. REP. (July 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/ [https://perma.cc/7NX6-4J6S] (summarizing recent state legislation expanding data protection).

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.[47] In fact, "[t]oday, the FTC is viewed as the de facto federal data protection authority."[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."[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.[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

47. Marc Rotenberg, *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* PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS, *supra* note 17, at 10, 10–11; Solove & Hartzog, *supra* note 11.

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." *Id.* at 598; Rotenberg, *supra* note 47, at 11; *Our History*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/our-history [https://perma.cc/BV6Y-DRKC].

49. 15 U.S.C. § 45; *see also A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/FBL2-DV4D] (Oct. 2019); FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017 (2018) [hereinafter FED. TRADE COMM'N 2017], https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf [https://perma.cc/WWJ3-UBC8]; Jessica Rich, Opinion, *Give the F.T.C. Some Teeth to Guard Our Privacy*, N.Y. TIMES (Aug. 12, 2019), https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html [https://perma.cc/3LWM-RCZJ]. The FTC has investigative and enforcement tools and broad jurisdiction under 15 U.S.C. § 45, but with some significant limits to its power. § 45; Chris Jay Hoofnagle et al., *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS: TECHTANK (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/XD8M-9JDW]. The FTC cannot set broad, normative privacy standards and cannot impose penalties on wrongdoers "unless they're already under an order for [a] previous wrongdoing . . . ." Rich, *supra*.

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.

invasive activities.[51] This privacy oversight is largely recognized as the notice-and-choice regime and offers much counsel for online practices.[52]

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.[53] 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."[54] Questions as to the actual scope of the FTC's powers have further muddied the waters.[55]

Meanwhile, at the state level, most privacy and tort laws have historically been ineffective at addressing these emerging digital problems.[56] But because of little progress made on a federal law, many states have started taking matters into their own hands.[57]

---

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.

53. *Retail Tracking Firm Settles FTC Charges It Misled Consumers About Opt Out Choices*, FED. TRADE COMM'N (Apr. 23, 2015) [hereinafter *Retail Tracking Firm*], https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers [https://perma.cc/E93M-BHE3] ("The complaint is the FTC's first against a retail tracking company.").

54. *See* William R. Denny, *Cybersecurity As an Unfair Practice: FTC Enforcement Under Section 5 of the FTC Act*, A.B.A. (June 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/06/cyber_center_denny [https://perma.cc/MC5P-2UUM].

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 torts 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).

57. Adam Stone, *As Privacy Concerns Grow, States Create Bold Policies*, GOV'T TECH. (July–Aug. 2019), https://www.govtech.com/policy/As-Privacy-Concerns-Grow-States-Create-Bold-Policies.html [https://perma.cc/Y2RU-2BPM] (quoting Washington Senator Reuven Carlyle as saying that "the federal government has made themselves functionally irrelevant," and noting that rather than wait anymore, Senator Carlyle and other state leaders are stepping up to assert control over the issue); Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, IAPP, https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/B9QQ-E6SR] (Mar. 3, 2021); Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 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.[58] The CCPA essentially grants consumers an exclusive right to privacy regarding all of their personal information.[59] Like the GDPR, which recognizes privacy and the protection of personal data as fundamental human rights, the CCPA provides strong protections for consumers.[60] 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.[61]

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.[62] However, the costs of compliance and risk of error in navigating fifty unique state laws along with any applicable federal and foreign laws could

---

https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html [https://perma.cc/Z3B2-RKKN]; Grande, *supra* note 13; Bennett Cyphers, *Big Tech's Disingenuous Push for a Federal Privacy Law*, EFF (Sept. 18, 2019), https://www.eff.org/deeplinks/2019/09/big-techs-disingenuous-push-federal-privacy-law [https://perma.cc/8XF4-8AWF].

58. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/NN77-US3U] ("The bill raced through the State Legislature without opposition on [June 28th] and was signed into law by Gov. Jerry Brown, just hours before a deadline to pull from the November ballot an initiative seeking even tougher oversight over technology companies."); Katelyn Ringrose & Jeremy Greenberg, *California Privacy Legislation: A Timeline of Key Events*, FUTURE OF PRIVACY F., https://fpf.org/2020/07/01/california-privacy-legislation-a-timeline-of-key-events/ [https://perma.cc/Q4G7-Y6PQ] (Aug. 31, 2020) (showing by timeline the short window within which legislators rushed to pass the CCPA to head off a stricter ballot initiative).

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.

61. *See* Michele Cohen, *The California Privacy Rights Act of 2020 Passed, Now What?*, JD SUPRA (Nov. 6, 2020), https://www.jdsupra.com/legalnews/the-california-privacy-rights-act-of-57046/ [https://perma.cc/8JGE-2DMA].

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.[63] Multiple conflicting laws would also create confusion and inconsistent outcomes for consumers as they shop locally, online, and across the country.[64] Stricter online protections also raise additional questions about how these laws would apply to brick-and-mortar.[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.[66] As such, a dire need for more uniform direction concerning information privacy exists, particularly in the brick-and-mortar context.[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.[68] To this end, more than a dozen bills and

63. *See generally* Grande, *supra* note 13.

64. Beckerman, *supra* note 57.

65. *See* McKinnon, *supra* note 5; McDowell et al., *supra* note 15 (highlighting existing ambiguity as to brick-and-mortar obligations); Andrew Burt, *Why Privacy Regulations Don't Always Do What They're Meant To*, HARV. BUS. REV.: SEC. & PRIV. (Oct. 23, 2018), https://hbr.org/2018/10/why-privacy-regulations-dont-always-do-what-theyre-meant-to [https://perma.cc/GC4Z-RL9U] (explaining that, in the context of the GDPR, a challenge with overly broad and generic regulations is that they treat all organizations the same and fail to include explicit recommendations or specific prohibitions in a way that is immediately clear for all companies).

66. TUROW, *supra* note 15; BUREAU OF THE CENSUS, U.S. DEP'T OF COM., CB20-120, QUARTERLY RETAIL E-COMMERCE SALES 2ND QUARTER 2020, at 2 tbl.1 (2020).

67. *See generally* Beckerman, *supra* note 57 (explaining that a patchwork of state laws are becoming more convoluted, benefiting only lawyers and the data compliance industry); Grande, *supra* note 13 (highlighting growing businesses' vulnerability to a complex and inconsistent regulatory environment with increased state regulation); McDowell et al., *supra* note 15 (noting uncertainty as to whether notice-and-choice applies in the brick-and-mortar context); Comment Letter from David French, Senior Vice President, Nat'l Retail Fed'n, to David J. Redl, Assistant Sec'y for Commc'ns & Info., Nat'l Telecomms. & Info. Admin. 3 (Nov. 9, 2019) [hereinafter NRF Comment Letter], https://www.ntia.doc.gov/files/ntia/publications/nrf_comments_to_ntia_re_consumer_privacy_submitted_9_nov_2018.pdf [https://perma.cc/85S9-VLWY] (emphasizing concern for the risk of misjudging different state laws that brick-and-mortar stores absorb in trying to serve their customers).

68. Grande, *supra* note 13 (observing support from the business community, including the U.S. Chamber of Commerce, The Software Alliance, and tech giants such as Google, Microsoft, and Apple); Rich, *supra* note 49 (highlighting the push for a broad, nationwide privacy standard among consumer advocates, industry leaders, and the FTC since the late 1990s); Cyphers, *supra* note 57 (observing that after years of fighting any kind of privacy legislation, big tech companies are now looking to the federal

discussion drafts targeting more comprehensive online privacy reform were circulated in the 116th Congress.[69] 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.[70]

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).

69. SAFE DATA Act, S. 4626, 116th Cong. (2020); Data Protection Act of 2020, S. 3300, 116th Cong. (2020); Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019); Information Transparency & Personal Data Control Act, H.R. 2013, 116th Cong. (2019); Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019); Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (2019); ADD Act, S. 142, 116th Cong. (2019); Social Media Privacy Protection and Consumer Rights Act of 2019, S. 189, 116th Cong. (2019); DATA Privacy Act, S. 583, 116th Cong. (2019); BROWSER Act of 2019, S. 1116, 116th Cong. (2019); Birnbaum, *supra* note 40 (discussing that the House Energy and Commerce Committee circulated the discussion draft of bipartisan federal privacy legislation); S. COMM. ON COM., SCI. & TRANSP., UNITED STATES CONSUMER DATA PRIVACY ACT OF 2019 DISCUSSION DRAFT (2019) [hereinafter USCDPA], https://aboutblaw.com/NaZ [https://perma.cc/V42B-LJ2H]; S. COMM. ON BANKING, HOUS., & URB. AFF., DATA ACCOUNTABILITY AND TRANSPARENCY ACT OF 2020 (2020), https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf [https://perma.cc/KC64-4ZUG].

70. *See generally, e.g.*, *Examining Legislative Proposals to Protect Consumer Data Privacy: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2019); *Protecting Consumer Privacy in the Era of Big Data: Hearing Before Subcomm. on Consumer Prot. & Com. of the H. Comm. on Energy & Com.*, 116th Cong. (2019); *Legislation*, INTEL [hereinafter *Intel Legislation*], https://usprivacybill.intel.com/legislation [https://perma.cc/9HCL-NS5X]; *Privacy for America Releases Detailed Policy Framework to Provide Strong Data Privacy Protections for All Americans*, PRIV. FOR AMERICA (Dec. 3, 2019), https://www.privacyforamerica.com/detailed-policy-framework-to-provide-strong-data-privacy-protections/ [https://perma.cc/P434-TZFG]; SENATE DEMOCRATS, PRIVACY AND DATA PROTECTION FRAMEWORK, https://www.democrats.senate.gov/imo/media/doc/Final_CMTE%20Privacy%20Principles_11.14.19.pdf [https://perma.cc/JA7D-NP24] (outlining the Senate Democratic leaders privacy principles); CTR. FOR DEMOCRACY & TECH., CDT FEDERAL BASELINE PRIVACY LEGISLATION DISCUSSION DRAFT (Dec. 5, 2018) [hereinafter CDT FEDERAL BASELINE], https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf [https://perma.cc/CJF4-FGU3].

notice-and-choice model.[71] 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.[72] 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.[73] The bills and proposals would also generally minimize data collection and put information safeguards in place.[74] Additionally, despite PII's conceptual problems, lawmakers in the 116th Congress widely agreed that some concept of PII is necessary moving forward.[75]

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).

73. *See* Ryan Moshell, *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 383 (2005); Alex Propes, *Privacy & FTC Rulemaking Authority: A Historical Context*, IAB (Nov. 6, 2018), https://www.iab.com/news/privacy-ftc-rulemaking-authority-a-historical-context/ [https://perma.cc/MF3R-BLCS].

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.[76] 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).[77] Notably, the deceptively subtle differences between these two approaches could present very different outcomes for brick-and-mortar tracking technologies.[78]

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."[79] These issues include private rights of action and preemption of state laws.[80] Preemption is of particular concern in brick-and-mortar privacy rhetoric.[81]

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."[82] 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.

79. Cameron F. Kerry, *Game On: What to Make of Senate Privacy Bills and Hearing*, BROOKINGS: TECHTANK (Dec. 3, 2019), https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/ [https://perma.cc/8799-TAQE].

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.[83] 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.[84]

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.[85] 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.[86] 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."[87]

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.[88] This oversight has since grown into some general parameters around the notice-and-choice requirement.[89] Vague language, technically correct but incomplete language, and language hidden in dense boilerplate policies have all been deemed insufficient for notice purposes.[90]

Further, even if no notice is given, and thus no promise is broken, the FTC has taken a stance against surreptitious consumer

83. *Id.*
84. *Id.* at 592, 604.
85. *Id.* at 592. *See generally* Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIV. F., https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-informatio n-practices/ [https://perma.cc/43LZ-P9JB] (Dec. 19, 2007) (discussing the FIPs of the HEW report and a list of the eight expanded principles codified in the OECD Guidelines of 1980).
86. Hoofnagle, *supra* note 4.
87. Solove & Hartzog, *supra* note 11, at 592–93.
88. *Id.* at 604.
89. *See id.*
90. *See id.* at 634–36.

surveillance online.[91] In *In re Aspen Way Enterprises, Inc.*, the FTC found that installing spyware and gathering data without notice was an unfair practice.[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."[93]

In the specific context of brick-and-mortar tracking, the FTC has handled only one case.[94] In *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.[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.[96]

However, several issues take shape in *In re Nomi*.[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.[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

91. *Id.* at 641.

92. *See* Complaint at 4, *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.

93. Solove & Hartzog, *supra* note 11, at 641 (quoting *Aspen* Complaint, *supra* note 92, at 2).

94. *Retail Tracking Firm*, *supra* note 53.

95. Complaint at 2–3, *In re* Nomi Techs., Inc., FTC File No. 132-3251 (F.T.C. Aug. 28, 2015) (No. C-4538).

96. *Id.*

97. *See generally* Dissenting Statement of Commissioner Joshua D. Wright, *In re Nomi*, FTC File No. 132-3251 (F.T.C. Sept. 12, 2015) (No. C-4538) [hereinafter Dissenting Statement of Commissioner Wright]; Tim Sparapani, *Privacy and Security Innovation: The Cautionary Tale of Nomi Technologies and the FTC*, FORBES (May 26, 2015, 11:46 AM), https://www.forbes.com/sites/timsparapani/2015/05/26/privacy-and-security-innovation-the-cautionary-tale-of-nomi-technologies-and-the-ftc/#64b31d9b4a38 [https://perma.cc/77K4-6C56].

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.[99]

2. Implications for Brick-and-Mortar

The puzzling result in *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.[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.[101]

The *In re Nomi* decision is also particularly troubling given brick-and-mortar retail's painful three-dimensional constraints that significantly stunt speed-to-market.[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.[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.[104] As such, it is unsurprising that bigger

99. Dissenting Statement of Commissioner Wright, *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, *supra* note 97.

100. *See* Sparapani, *supra* note 97.

101. Dissenting Statement of Commissioner Wright, *supra* note 97, at 1 (pointing out that even if the facts of the *In re Nomi* case did support a technical violation, prosecutorial discretion favored restraint); McDowell et al., *supra* note 15 (noting that the FTC's approach in *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, *supra* note 97 (hypothesizing that the effects of the *In re Nomi* order are "likely" to extend to all businesses).

102. *See* NISSENBAUM, *supra* note 4, at 29.

103. *See A Guide to Retail Print Graphics*, THE VOMELA COS., https://info.vomela.com/guide-to-retail-print-graphics-windows-walls-floors?_ga=2.147550967.1931912370.1608421784-1571079601.1608421784 [https://perma.cc/G83V-W8WS].

104. *See, e.g.*, THE VOMELA COS., PETCO DOG TREAT PROJECT 2, https://cdn2.hubspot.net/hubfs/1689179/Case%20Studies/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]

---

105. Ruff, *supra* note 22 (describing how big-box home improvement retailer Lowe's created its innovation lab in 2015 to test concepts that rolled out *several years* later). The cashierless Amazon Go store offers another example of the timing and difficulty associated with a larger store-of-the-future rollout—the new store was announced in December 2016 with plans to open to the public in "early 2017," but due to "kinks" with the technology, the opening was ultimately pushed back almost a year. Laura Stevens, *Amazon Delays Opening of Cashierless Store to Work Out Kinks*, WALL ST. J.: TECH (Mar. 27, 2017, 10:41 AM), https://www.wsj.com/articles/amazon-delays-convenience-store-opening-to-work-out-kinks-1490616133 [https://perma.cc/H94L-EC6Q]; Matt Day, *Amazon Go Cashierless Convenience Store Opens to the Public in Seattle*, SEATTLE TIMES, https://www.seattletimes.com/business/amazon/amazon-go-cashierless-convenience-store-opening-to-the-public/ [https://perma.cc/7GZE-WA4M] (Jan. 22, 2018, 9:54 PM).

106. *See* WALKBASE, *supra* note 7, at 17–20.

107. *Id.*

108. *See* NRF Comment Letter, *supra* note 67, at 4.

109. *See* Dissenting Statement of Commissioner Wright, *supra* note 97, at 4 (explaining that the aggressive prosecution of Nomi "[sent] a dangerous message to [businesses] weighing the costs and benefits of voluntarily providing information and choice to consumers"); McDowell et al., *supra* note 15; Sparapani, *supra* note 97; McKinnon, *supra* note 5.

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.[111] 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.[112] 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.[113]

Under this approach, privacy cannot be left to self-regulation when businesses have such substantial profit incentives.[114] 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.[115]

Impact on Competition and Innovation: Hearing Before the S. Comm. on the Judiciary, 116th Cong. 3–4 (2019) (statement of Jane Bambauer, Professor of Law, University of Arizona) [hereinafter *Bambauer Statement*] (referencing a property model and a harm- or risk-based approach).

111. *Bambauer Statement*, *supra* note 110, at 3. *See generally* Press Release, Sen. Maria Cantwell, Cantwell, Senate Democrats Unveil Strong Online Privacy Rights (Nov. 26, 2019), https://www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights [https://perma.cc/T98G-MGVL].

112. *See generally* Press Release, *supra* note 111; *Bambauer Statement*, *supra* note 110, at 3.

113. *Bambauer Statement*, *supra* note 110, at 3; S. 3300, 116th Cong. (2020); *see also California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST.: OFF. OF THE ATT'Y GEN., https://oag.ca.gov/privacy/ccpa [https://perma.cc/LUD8-NBA3]; Letter from Alastair Mactaggart to Initiative Coordinator, California Off. of the Att'y Gen. (Nov. 4, 2019) [hereinafter Mactaggart Letter], https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf [https://perma.cc/CZ6U-MVSJ].

114. *See* Mactaggart Letter, *supra* note 113; *see also* Lily Hay Newman, *Never Trust a Platform to Put Privacy Ahead of Profit*, WIRED: SECURITY (Oct. 9, 2019, 2:32 PM), https://www.wired.com/story/twitter-two-factor-advertising/ [https://perma.cc/FFF3-RDZ7] (using examples of several big companies pulling phone numbers and other data used for two-factor authentication into their marketing databases to show that big companies are not prioritizing user privacy and security ahead of their business goals, despite having the resources to easily control and protect this data).

115. *See* Press Release, *supra* note 111; Kerry, *supra* note 71; *Bambauer Statement*, *supra* note 110, at 3; *see also, e.g.*, S. 1214, 116th Cong. § 17(a)(1) (2019) ("Any individual alleging a violation . . . may bring a civil action in any court of competent jurisdiction."); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 301(c)(1) (2019) ("Any individual alleging a violation . . . may bring a civil action in any court of competent jurisdiction, State or Federal."); CAL. CIV. CODE § 1798.150(a)(1) (West 2020) (authorizing consumers to bring civil suits for statutory damages).

Many of these models continue to rely heavily on notice and consent before or during collection of PII, with limited exemptions.[116] 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.[117]

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.[118] 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.[119]

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.[120] 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

116. Cameron F. Kerry & Caitlin Chin, *Hitting Refresh on Privacy Policies: Recommendations for Notice and Transparency*, BROOKINGS: TECHTANK (Jan. 6, 2020), https://www.brookings.edu/blog/techtank/2020/01/06/hitting-refresh-on-privacy-policies-recommendations-for-notice-and-transparency/ [https://perma.cc/5QUQ-37CC]; *see also, e.g.*, Online Privacy Act of 2019, H.R. 4978, 116th Cong. § 212 (2019); Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. § 3(b); S. 2968 §§ 102(b), 105(b)–(c) (2019).

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").

119. *See, e.g.*, H.R. 4978 §§ 101–107; S. 3456 §§ 4, 5.

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.[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.[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.[123] And this feat becomes even more difficult and complex when a bill bans this identification process.[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.[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.[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.[127]

Likewise, a laundry list of unlimited consumer rights may also pose some unintended consequences. Data portability, for example,

121. Schwartz & Solove, *supra* note 36, at 1829, 1832, 1871–72.

122. *Id.* at 1829 (noting that these types of definitions are unhelpful for distinguishing PII from non-PII); *see also* RILA Comment Letter, *supra* note 68, at 2.

123. Schwartz & Solove, *supra* note 36, at 1876–77.

124. *See, e.g.*, H.R. 4978 § 206.

125. NRF Comment Letter, *supra* note 67, at 3; *see also* James Campbell et al., *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47, 47, 49 (2015) (demonstrating that compliance costs from privacy regulation will disproportionately burden smaller firms and new firms and proposing that "the impact on market structure should be an important part of the discussion on privacy regulation").

126. CAL. CIV. CODE § 1798.140 (West 2020).

127. Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of $55 Billion to Get in Compliance*, CNBC: TECH, https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html [https://perma.cc/4JTD-39UV] (Oct. 8, 2019, 10:38 AM).

could breed anticompetitive outcomes.[128] 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.[129]

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."[130] 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."[131] 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.[132] 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.[133]

---

128. RILA Comment Letter, *supra* note 68, at 2.

129. *See generally* JAMES PAVUR & CASEY KNERR, BLACKHAT, GDPARRRRR: USING PRIVACY LAWS TO STEAL IDENTITIES (2019), https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf [https://perma.cc/9YAR-56G3].

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.[147] Elements of business behavior are also beginning to appear in consumer control models.[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.[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.[150] Long-running, irreconcilable differences have shown that no solution will elegantly resolve these competing interests.[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.[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.[153] Recent events, including a string of data breaches, the passage of strict privacy laws in Europe and California, and pressure from

147. *See Bambauer Statement*, *supra* note 110, at 6.
148. Kerry, *supra* note 71.
149. *See generally* Press Release, *supra* note 111.
150. Altshuler, *supra* note 4.
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").
152. *See* Kerry, *supra* note 13.
153. *See, e.g.*, 15 U.S.C. §§ 6501–6506.

consumers, have renewed interest in a federal privacy law and may have created the perfect incubator for its passage.[154]

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.[155] In response to delayed federal action, state governments are moving to pick up the privacy torch.[156] 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.[157] 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.[158]

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.[159]

---

154. Birnbaum, *supra* note 40 (noting efforts to develop a bipartisan federal privacy bill); Rich, *supra* note 68; Daniel R. Stoller & Ben Brody, *New FTC Powers Weighed in Senate Data Privacy Hearing*, BLOOMBERG L.: PRIV. & DATA SEC. L. NEWS (Feb. 27, 2019, 2:28 PM), https://news.bloomberglaw.com/privacy-and-data-security/new-ftc-powers-weighed-in-senate-data-privacy-hearing-1 [https://perma.cc/5KLT-NUSV].

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

(May 11, 2018, 6:39 AM), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html [https://perma.cc/6QN7-X92H] (describing the fatal impact of the cost of complying on smaller businesses in the context of the GDPR); Campbell et al., *supra* note 125, at 47; Feiner, *supra* note 127.

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

161. *Bambauer Statement*, *supra* note 110, at 2.

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.[166] Further, a federal law could actually provide stronger, more comprehensive protections that eliminate gaps in state laws and issues with patchwork compliance.[167]

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.[168] 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.[169] 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.[170]

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-U24P] (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.

168. *Latest Study Shows Heightened Importance of Retail to the U.S. Economy*, NAT'L RETAIL FED'N: ECON. (July 20, 2020) (citing NAT'L RETAIL FED'N & PRICEWATERHOUSECOOPERS LLP, THE ECONOMIC IMPACT OF THE US RETAIL INDUSTRY (2020)), https://nrf.com/blog/latest-study-shows-heightened-importance-retail-us-economy [https://perma.cc/8NX3-C5ZQ]; *Gross Domestic Product, Fourth Quarter and Year 2019 (Advance Estimate)*, BUREAU OF ECON. ANALYSIS (Jan. 30, 2020) [hereinafter *GDP Q4 2019*], https://www.bea.gov/news/2020/gross-domestic-product-fourth-quarter-and-year-2019-advance-estimate [https://perma.cc/RS5T-UM2H].

169. BUREAU OF THE CENSUS, *supra* note 15; *NRF Says 'State of the Economy is Sound' and Forecasts Retail Sales Will Grow Between 3.8 and 4.4 Percent*, NAT'L RETAIL FED'N: ECON. (Feb. 5, 2019) [hereinafter *NRF Forecasts*], https://nrf.com/media-center/press-releases/nrf-says-state-economy-sound-and-forecasts-retail-sales-will-grow [https://perma.cc/6NX9-3CLH] (estimating retail sales at more than $3.8 trillion in 2019); *see also State of Retail*, NAT'L RETAIL FED'N: ECON., https://nrf.com/insights/economy/state-retail [https://perma.cc/WDJ6-WNLW] ("Of the top 50 online retailers, nearly all operate stores.").

170. *See* discussion *supra* Sections II.A.2, II.B.1.

that often take years to develop and roll out across physical retail locations.[171] 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.[172] 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.[173] 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.[174] 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.[175]

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.[176] 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.[177] 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.[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."[179] At first blush, consumer control models appear to provide consumers with the greatest protections.[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.[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.[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

178. NISSENBAUM, *supra* note 4, at 238.

179. Polina Arsentyeva, *It's 2019, So Why Are We Still Talking About Opt-In Consent?*, IAPP (Nov. 12, 2019), https://iapp.org/news/a/its-2019-so-why-are-we-still-talking-about-opt-in-consent/ [https://perma.cc/QT69-LCJE]; *see also* discussion *supra* Section II.A. *See generally* Kerry & Chin, *supra* note 116.

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.

consumer data, while using duties of care to allow flexibility and innovation to develop systems and processes that do not depend on intrusive surveillance.[183]

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.[184] Despite concerns that the FTC is not up to the task, no enforcement candidate seems better suited for the job.[185] The reality is that the FTC's legal authority over privacy is the same as it was before the internet.[186] 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.[187] 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.[188]

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.[189] As such, the FTC could take on many more cases and step up to lead the U.S. privacy regulatory effort if properly

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.").

184. *See generally* Hoofnagle et al., *supra* note 49.

185. *Id.*; *see also* Rich, *supra* note 49.

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).

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].

188. Hoofnagle et al., *supra* note 49; Rich, *supra* note 49.

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 . . . .").

equipped to do so.[190] 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.[191] 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.[192]

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.[193] To that end, some bills have sought to empower individuals with a PRA.[194] 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.[195]

---

190. *See generally* Hoofnagle et al., *supra* note 49.

191. *See generally* Rich, *supra* note 49.

192. Propes, *supra* note 73.

193. Emily Birnbaum, *FTC Dem: Regulators Are 'Drinking the Kool-Aid' of Monopolists*, THE HILL (Nov. 14, 2019, 12:37 PM) (quoting FTC Commissioner Rohit Chopra), https://thehill.com/policy/technology/470488-ftc-dem-worries-regulators-drinking-the-kool-aid-of-monopolists [https://perma.cc/587J-MXXF]; *see also* Hoofnagle et al., *supra* note 49.

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.[196] 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.[197] 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.[198]

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.[199] 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."[200] Because of this malleable nature, broad definitions such as "linked or reasonably

---

TECHTANK (July 7, 2020), https://www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/ [https://perma.cc/3W93-P2P6] (explaining that despite polar positions on a PRA, a PRA is not an all-or-nothing proposition and proposing a tiered substantive rights approach as a possible way forward).

196. *See, e.g.*, USCDPA, *supra* note 69, at 20–22.

197. Stoller & Brody, *supra* note 154.

198. *See* U.S. CHAMBER INST. FOR LEGAL REFORM, ILL-SUITED: PRIVATE RIGHTS OF ACTION AND PRIVACY CLAIMS 19 (July 2019).

199. *See* RILA Comment Letter, *supra* note 68, at 2.

200. Schwartz & Solove, *supra* note 36, at 1846.

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.[205] 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.[206] 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.[207] 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.

206. *See* Jeff Glueck, Opinion, *How to Stop the Abuse of Location Data*, N.Y. TIMES (Oct. 16, 2019), https://www.nytimes.com/2019/10/16/opinion/foursquare-privacy-internet.html [https://perma.cc/T6Z9-V8U4].

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.[208]

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.[209] 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.[210] Consumers can also quickly become inundated by obvious or seemingly insignificant choices and become less attentive to choices that are important to them.[211]

---

208. ANN CAVOUKIAN, INFO. & PRIV. COMM'R OF ONT., CAN., WHITE PAPER: ANONYMOUS VIDEO ANALYTICS (AVA) TECHNOLOGY AND PRIVACY 2–4 (2011), https://www.ipc.on.ca/wp-content/uploads/Resources/AVAwhite6.pdf [https://perma.cc/5TR6-36XF].

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

210. Altshuler, *supra* note 4; Kerry & Chin, *supra* note 116; Charlie Warzel, Opinion, *Privacy Is Not Your Responsibility*, N.Y. TIMES (Sept. 17, 2019) (quoting Colin Horgan, *Tech Isn't Vulnerable—You Are*, ONEZERO (Sept. 4, 2019), https://onezero.medium.com/tech-isnt-vulnerable-you-are-de82b8102610 [https://perma.cc/EXJ5-BY3C]), https://www.nytimes.com/2019/09/17/opinion/alabama-app-privacy.html [https://perma.cc/WR7T-M46K].

211. Sheena S. Iyengar & Mark R. Lepper, *When Choice Is Demotivating: Can One Desire Too Much of a Good Thing?*, 79 J. PERSONALITY & SOC. PSYCH. 995, 996, 999 (2000) (first citing Ravi Dhar, *Consumer Preference for a No-Choice Option*, 24 J. CONSUMER RSCH. 215 (1997); then citing Eldar Shafir et al., *Reason-Based Choice*, 49 COGNITION 11 (1993); then citing Eldar Shafir & Amos Tversky, *Thinking Through Uncertainty: Nonconsequential Reasoning and Choice*, 24 COGNITION 449 (1992); then citing John R. Hauser & Birger Wernerfelt, *An Evaluation Cost Model of Consideration Sets*, 16 J. CONSUMER RSCH. 393 (1990); then citing John W. Payne, *Contingent Decision Behavior*, 92 PSYCH. BULL. 382 (1982); then citing John W. Payne et al., *Adaptive Strategy Selection in Decision Making*, 14 J. EXPERIMENTAL PSYCH.: LEARNING MEMORY & COGNITION 534 (1988); then citing JOHN W. PAYNE ET AL., THE ADAPTIVE DECISION MAKER (1993); then citing Danielle Timmermans, *The Impact of Task Complexity on Information Use in Multi-Attribute Decision Making*, 6 J. BEHAV. DECISION MAKING 95 (1993); and then citing Peter Wright, *Consumer Choice Strategies: Simplifying vs. Optimizing*, 12 J. MKTG. RSCH. 60 (1975)).

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.[212] 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.[213] Moreover, it creates a substantial and unnecessary privacy risk.[214]

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.[215]

4. Notice Through 21st Century Technology

Based on the bills and proposals before the 116th Congress, it is clear that notice or awareness continues to be a key concern.[216] 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.[217]

212. *Bambauer Statement*, *supra* note 110, at 6.

213. Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98. CALIF. L. REV. 1765, 1801–02 (2010).

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

218. FitzGerald, *supra* note 6; Nguyen, *supra* note 10; WORLD ECON. F., REDESIGNING DATA PRIVACY: REIMAGINING NOTICE & CONSENT FOR HUMAN-TECHNOLOGY INTERACTION 7 (2020), https://www.weforum.org/reports/redesigning-data-privacy-reimagining-notice-consent-for-humantechnology-interaction [https://perma.cc/BFV6-KM2X].

219. *See Our Company Privacy Policy*, GEN. DATA PROT. REGUL., https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf [https://perma.cc/Y8TA-WAS9].

220. Kerry & Chin, *supra* note 116 (detailing the benefits and workings of a two-tiered approach).

221. *Id.*

222. *See* Brian Kint, *Is It Time to Rethink Notice and Choice As a Fair Information Privacy Practice?*, CYBER L. MONITOR (Feb. 13, 2019), https://www.cyberlawmonitor.com/2019/02/13/is-it-time-to-rethink-notice-and-choice-as-a-fair-information-privacy-practice/ [https://perma.cc/ZY35-5KUD] (recommending a similar layered privacy notice and explaining how it would work).

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.[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.[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.[225] Alternatively, a standardized privacy-enhancing app could allow users to automatically disable signal transmission when approaching these networks to avoid collection altogether.[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.[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.[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.[229] The question is, thus, whether Congress will delay the

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).

224. *Id.*; *see also* Michael Grothaus, *How to Find Hidden Cameras in Your Airbnb, and Anywhere Else*, FAST CO. (Apr. 15, 2019), https://www.fastcompany.com/90331449/how-to-find-hidden-cameras-in-your-airbnb-and-anywhere-else [https://perma.cc/JC7R-BHS2] (explaining how Wi-Fi sniffing apps can be used to detect smart devices when Airbnb owners secretly hide cameras in rooms).

225. Soltani, *supra* note 9.

226. *Id.*

227. WORLD ECON. F., *supra* note 218, at 22–23.

228. *Id.* at 24.

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.[230] 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.[231] 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.[232] 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.[233] 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.[234] 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.