Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 29 *XXIX*
Number 2

Article 4

2019

Shopping For Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers

Vincent Nguyen
Fashion Law Institute at Fordham Law School, vincent@fashionlawinstitute.com

Shopping For Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers

Cover Page Footnote
Dean's Fellow for the Fashion Law Institute at Fordham Law School. I would like to thank my family and friends who have begrudgingly accepted my justification of shopping for the sake of academic research. Special thanks to Professors Susan Scafidi, Founder and Director of the Fashion Law Institute, Ari Ezra Waldman, Professor of Law and Director for the Innovation Center for Law and Technology at New York Law School; and Elizabeth Cooper, Professor at Fordham Law School and Director for the Feerick Center for Social Justice.

Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers

Vincent Nguyen*

As technology continues to rapidly advance, the American legal system has failed to protect individual shoppers from the technology implemented into retail stores, which poses significant privacy risks but does not violate the law. In particular, I examine the technologies implemented into many brick-and-mortar stores today, many of which the average everyday shopper has no idea exists. This Article criticizes these technologies, suggesting that many, if not all of them, are questionable in their legality taking advantage of their status in a legal gray zone. Because the American judicial system cannot adequately protect the individual shopper from these questionable privacy practices, I call upon the Federal Trade Commission, the de facto privacy regulator in the United States, to increase its policing of physical retail stores to protect the shopper from any further harm.

* Dean's Fellow for the Fashion Law Institute at Fordham Law School. I would like to thank my family and friends who have begrudgingly accepted my justification of shopping for the sake of academic research. Special thanks to Professors Susan Scafidi, Founder and Director of the Fashion Law Institute, Ari Ezra Waldman, Professor of Law and Director for the Innovation Center for Law and Technology at New York Law School; and Elizabeth Cooper, Professor at Fordham Law School and Director for the Feerick Center for Social Justice.

INTRODUCTION 536
I. AMERICAN PRIVACY REGULATION 539
II. EXAMPLES OF PRIVACY ISSUES PRESENTED BY RETAIL STORES 542
A. Facial Recognition 543
B. Beacon Technology 546
C. RFID Technology 549
D. The eStore 552
1. The Artificially Intelligent Stylist 553
2. Omnichannel 554
3. Dynamic Pricing 557
III. THE LAW LAGS BEHIND TECHNOLOGICAL ADVANCEMENTS WITH NO AVAILABLE JUDICIAL RECOURSE 559
IV. HOW INCREASED FTC REGULATION CAN PREVENT RETAIL STORES FROM INVADING SHOPPER'S PRIVACY 562
A. Prominent Notice 563
B. Opt-In Consent 564
C. Precise Location 565
D. Collection of Personal Information 566
E. Targeted Advertising 568
CONCLUSION 569

INTRODUCTION

The 2016 Met Gala exhibition, "Manus x Machina: Fashion in an Age of Technology," examined the relationship between technology and fashion.[1] The exhibit featured clothing, designs, and technology, from dresses made by sewing machine to 3D printing, recognizing that technology has consistently energized the fashion

[1] *See* Imran Amed & Lauren Sherman, *Decoding 'Manus x Machina'*, BUS. OF FASHION (May 3, 2016, 5:30 AM), https://www.businessoffashion.com/articles/intelligence/manus-x-machina-met-gala-apple-costume-institute-anna-wintour-andrew-bolton-jony-ive [https://perma.cc/K7YE-MXKZ] (noting curator Andrew Bolton's comment that "[f]ashion has always been the first to embrace technology, right from the get go").

industry.[2] In the time since the exhibit, the retail industry has continued to incorporate technology into the shopping and retail experience. However, these technological advances and their subsequent implementation have created significant privacy issues for consumers, many of which remain virtually unknown and undisclosed to the ordinary shopper.

Tim Cook, the chief executive officer of Apple, has cautioned against the "data industrial complex" where "[o]ur own information—from the everyday to the deeply personal—is being weaponized against us with military efficiency."[3] He described the "billions of dollars [that] change hands, and countless decisions [that] are made, on the basis of our likes and dislikes, our families and friends, our relationships and conversations . . . [o]ur wishes and fears, our hopes and dreams."[4] The retail industry both capitalizes on and actively participates in this data industrial complex, increasingly using technology and consumer information to market, advertise, and sell products.[5] In fact, much of the technology

---

[2] *See, e.g.*, *"Remote Control,"* Heilbrunn Timeline of Art History, THE METROPOLITAN MUSEUM OF ART (2019), https://www.metmuseum.org/toah/works-of-art/2006.251a-c/ [https://perma.cc/W8W5-TJLH] (describing a "remote control" dress designed by Hussein Chalayan as a commentary on contemporary society and culture); Naomi Shavin, *Iris Van Herpen Is Revolutionizing the Look and Tech of Fashion*, SMITHSONIAN (May 2, 2016), https://www.smithsonianmag.com/arts-culture/iris-van-herpen-revolutionizing-look-and-tech-fashion-180958969/ [https://perma.cc/ELV4-NMPF] (describing the 3D printing technique to create garments comparable to living organisms); Tom Warren, *Apple Watch Series 4 Includes a Bigger Display and a Built-in EKG Scanner*, THE VERGE (Sept. 12, 2018, 1:11 PM), https://www.theverge.com/2018/9/12/17847086/new-apple-watch-series-4-price-features-release-date-2018 [https://perma.cc/N4DX-ZGLT] (describing the new features offered in the fourth generation of Apple Watch, perhaps the most obvious example of technology encroaching on the fashion sector).

[3] *See* Natasha Lomas, *Apple's Tim Cook Makes Blistering Attack on the 'Data Industrial Complex'*, TECHCRUNCH (Oct. 24, 2018), https://techcrunch.com/2018/10/24/apples-tim-cook-makes-blistering-attack-on-the-data-industrial-complex/ [https://perma.cc/J9AA-UMKS].

[4] *See* Sara Salinas & Sam Meredith, *Tim Cook: Personal Data Collection is Being "Weaponized Against Us With Military Efficiency,"* CNBC (Oct. 24, 2018, 6:22 AM), https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html [https://perma.cc/8P4A-FR55].

[5] *See, e.g.*, Arthur Zaczkiewicz, *Retail Success Hinges on Using Technology and Data – With a Strategy,* WOMEN'S WEAR DAILY (May 8, 2018), https://wwd.com/business-news/technology/retail-technology-1202667884/ [https://perma.cc/2C4G-EFH2] (quoting

retailers incorporate into their physical stores outpaces the law, operating in a legal gray zone.[6] As a result, the American legal system neither recognizes nor timely responds to these developing privacy issues because the traditional privacy torts are inapplicable.[7] As the de facto privacy regulator in the United States, the Federal Trade Commission ("FTC") can respond to these privacy concerns, but remains handicapped by insufficient resources and continually evolving technology.[8] Fortunately, based on an analysis of previous enforcement actions, which usually result in settlement, prosecution, or other injunctive remedies, the FTC appears willing to protect shoppers' privacy.[9] Therefore, this Article recommends the FTC increase its policing of the technology found in traditional brick-and-mortar retail stores.[10]

Part I describes the current American privacy regime in the United States, focusing primarily on the FTC, which operates as its de facto privacy regulator. Part II provides specific examples of technologies implemented into retail stores. The shopper first encounters technologies, which may infringe upon their privacy when entering the store. Facial recognition technology can photograph the shopper's face and acquire their biometric information. After entrance, the store can use beacon and radio frequency identification ("RFID") technology to track customers and products. Stores can then use technology to manipulate the shopper into pur-

---

various data and technology company representatives describing how analysis of data aids retailers to sell products); Richard Kestenbaum, *This Is What the Retail Industry Is Talking About Now*, FORBES (Jan 28, 2018), https://www.forbes.com/sites/richardkestenbaum/2018/01/28/this-is-what-the-retail-industry-is-talking-about-now/#50b2d0e37680 [https://perma.cc/7RBS-BR82] (describing the National Retail Federation Big Show, which increasingly emphasized the experiential retail store's implementation of new technology).

6 Kati Chitrakorn, *5 Technologies Transforming Retail in 2018*, BUS. OF FASHION (Jan 19, 2018), https://www.businessoffashion.com/articles/fashion-tech/5-technologies-transforming-retail [https://perma.cc/QK7P-JLFD] (identifying artificial intelligence, augmented reality, blockchain, contactless shopping, and facial recognition as the technologies shaping the retail and shopping experience). Though these relatively new technologies have existed for a few years, technological developments consistently outpace the law. *See infra* Part I.

7 *See infra* Part I; *see infra* Part III.

8 *See infra* Part I.

9 *See infra* Part I; *see also infra* Section IV.A.

10 *See infra* Part IV.

chasing items via artificial styling,[11] omnichannel shopping,[12] and dynamic pricing.[13] Part III identifies the primary privacy issue presented by the technologies described in Part II, exacerbated by the courts' inability to regulate issues of retail privacy. Finally, Part IV advocates for increased FTC involvement in the physical retail space examining prior FTC decisions, which indicate the FTC is willing to protect individual consumers from retail stores invading their privacy.

I. AMERICAN PRIVACY REGULATION

Privacy regulation in the United States consists of an ineffective blend of agency guidance, common and constitutional law, and industry-specific regulations.[14] Consequently, the FTC operates as the de facto privacy regulator to address the gaps created by these different legal sources.[15] Though Congress first established the FTC to ensure fair competition in commerce, its regulatory authority eventually increased to also include consumer privacy.[16] In 1938, Congress amended Section 5 of the Federal Trade Commission Act, expanding the FTC's jurisdiction "to prohibit 'unfair or deceptive' acts or practices."[17] The FTC uses this authority to assert claims against "unfair or deceptive acts or practices in or affecting commerce."[18] An "unfair" or "deceptive" act or practice

---

11 *See infra* Section II.D.

12 *See infra* Section II.D.

13 *See infra* Section II.D.

14 *See* Jorge L. Contreras, *Genetic Property*, 105 GEO. L.J. 1, 15 (2016).

15 Daniel Solove and Woodrow Hartzog describe how the FTC became the "de facto" American privacy regulator. Solove and Hartzog argue that the FTC complaints, settlements, and enforcement actions act as common law for informational privacy in the United States. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 604 (2014).

16 *See id.* at 598.

17 Section 5 of the FTC Act is titled "[u]nfair methods of competition unlawful; prevention by Commission." 15 U.S.C. § 45 (2012).

18 15 U.S.C. § 45(a)(1) (2012); *see also* Federal Trade Commission Act of 1914, ch. 311, 38 Stat. 717, 15 U.S.C. §§ 41–58 (1914); FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 610–12 (D.N.J. 2014) (rejecting the argument that the FTC does not have authority to regulate privacy through enforcement actions), *aff'd*, 799 F.3d 236 (3d Cir. 2015). The FTC began by focusing on "deceptive" trade practices, though it gradually

"causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[19] The FTC uses the authority provided by Section 5 to police a range of actors, activities, and industries,[20] except where a regulation exclusively governs a particular industry such as healthcare or children.[21]

The FTC acts mostly by identifying and policing violations of the FTC Act.[22] Due to its lack of rulemaking authority, the FTC initially encouraged industries to self-regulate, only enforcing what a company or industry explicitly promised.[23] In other words, instead of the FTC creating rules, companies would create their own rules, and the FTC would hold them accountable.[24] As a result, most companies avoided making explicit promises and the FTC's public statements amounted to little more than recommendations.[25] Beyond general data security requirements, as long as a company's privacy policy notified consumers about its data collection policies, the FTC refrained from micromanaging privacy concerns be-

---

began to file complaints against companies under the "unfair" trade practices rationale. *See* Solove & Hartzog, *supra* note 15, at 599.

19 15 U.S.C. § 45(n) (2012).

20 *See* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 964–66 (2016) (describing the breadth of FTC authority across industries asserting that "[i]ts unfairness authority is the broadest portion of the Commission's statutory authority").

21 *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, 110 Stat. 1936 (1996); *see also* Children's Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105–277, 112 Stat. 2681–729, 15 U.S.C. §§ 6501-6506 (1998).

22 *See* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 130–31 (2008).

23 *See* Solove & Hartzog, *supra* note 15, at 599.

24 *Id.* at 598.

25 *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/V6XF-KPZG]. However, this notice-and-choice model results in companies posting long privacy policies unintelligible to the average consumer (if read at all). *See id*.

tween parties.[26] However, between 1995 and 2000, the FTC further expanded its regulatory powers.[27]

Though Section 5 does not expressly mention individual privacy, the FTC broadly interprets Section 5 to apply to a person's information privacy, data security, consumer data, tracking, and related business activities.[28] Unfortunately, Section 5 contains outdated language, failing to even include the terms "privacy" or "technology," presenting obvious additional hurdles.[29] Fortunately, the FTC best applies this outdated language to developing privacy issues and technologies.[30] Ultimately, the FTC uses this Section 5 authority to ensure consumers receive fair information practices such as: notice, choice, access, accuracy, data minimization, security, and accountability.[31]

While the FTC has broad subject-matter jurisdiction under Section 5, the FTC has relatively few enforcement tools.[32] When bringing an enforcement action against a company, the FTC first identifies conduct believed to be deceptive or unfair, usually at the recommendation of a concerned or aggrieved party. This complaint serves either as the basis for a later settlement or the initiation of administrative or federal litigation.[33] Through settlement or successful prosecution, the FTC can obtain certain injunctive remedies such as fines, injunctions on infringing activities, and modifications to existing business practices.[34] A final settlement order typically contains common provisions, which restrict the infringing

---

26 *See* Solove & Hartzog, *supra* note 15, at 603.

27 *Id.* at 604.

28 *See id.* at 598 (describing the "dawn of FTC privacy enforcement" stemming from this broad interpretation and enforcement of Section 5).

29 *See* 15 U.S.C. § 45 (2006).

30 *See* Solove & Hartzog*, supra* note 15, at 587.

31 *See id.* at 592–93.

32 *See* Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U. L. REV. 1183, 1209 (2017) ("The FTC is limited to Magnuson-Moss rulemaking authority under section 5, which effectively leaves the FTC with two means to advance an information privacy agenda: namely, enforcement of violations of section 5 and informal guidance, including guidance published in the Code of Federal Regulations but lacking the formal nature of rulemaking.").

33 *See id.*

34 *See* Solove & Hartzog, *supra* note 15, at 610–19.

party's activities.[35] Ultimately, the FTC is viewed as the de facto data protection authority in the United States. In fact, many privacy lawyers and companies view the FTC as a formidable enforcement authority, analyzing FTC statements, decisions, and settlement orders.[36] Because of its broad authority over interstate commerce, the FTC is tasked with addressing the privacy concerns presented by technology within the retail industry, an additional responsibility on an overburdened federal agency.

II. EXAMPLES OF PRIVACY ISSUES PRESENTED BY RETAIL STORES

Though countless articles bemoan the death of physical retail,[37] brick-and-mortar stores continue to flourish, adapting and implementing technology to compete with their online counterparts.[38] This Part details the privacy issues consumers may encounter during the shopping experience: from their initial entrance to the store, to the point of purchase, and even after departure.[39] Upon entry, facial recognition technology can photograph a shopper's face and

---

35 *See* Brill & Jones, *supra* note 322, at 1209 ("[T]he resulting order typically contains certain commitments binding the defendant: injunctive relief against continued violations, compliance and reporting obligations, recordkeeping requirements, employee acknowledgment of the order, and, in some cases, equitable monetary relief (e.g., disgorgement).").

36 *See* Solove & Hartzog, *supra* note 15, at 620.

37 *See, e.g.*, Wolf Richter, *The Retail Apocalypse Keeps Killing Brick and Mortar Stores*, BUS. INSIDER (Feb. 4, 2018, 7:32 AM), https://www.businessinsider.com/the-retail-apocalypse-keeps-killing-brick-and-mortar-stores-2018-2 [https://perma.cc/VRS6-J5MD]; Robert Klara, *Bad News, Brick-and-Mortar Stores: The Internet Finally Has You Beat*, ADWEEK (Nov. 11, 2017), https://www.adweek.com/brand-marketing/bad-news-brick-and-mortar-stores-the-internet-finally-has-you-beat/ [https://perma.cc/D7PA-KLQT]; Derek Thompson, *What in the World Is Causing the Retail Meltdown of 2017?*, THE ATLANTIC (Apr. 10, 2017), https://www.theatlantic.com/business/archive/2017/04/retail-meltdown-of-2017/522384/ [https://perma.cc/3627-8Z4J].

38 *See* Darrell K. Rigby, *The Future of Shopping*, HARV. BUS. REV. (Dec. 2011), https://hbr.org/2011/12/the-future-of-shopping [https://perma.cc/EUN9-JK4Y]; *see also* Michelle Evans, *New Technologies That Will Change How Consumers Shop In Store,* FORBES (Jan. 18, 2018, 12:19 PM), https://www.forbes.com/sites/michelleevans1/2018/01/18/new-technologies-that-will-change-how-consumers-shop-in-store/#251c972b5fc9 [https://perma.cc/QK5L-EGYU].

39 Elizabeth Paton, *Imagining the Retail Store of the Future*, N.Y. TIMES (Apr. 12, 2017), https://www.nytimes.com/2017/04/12/fashion/store-of-the-future.html [https://perma.cc/U3WK-ZAZJ].

acquire their unique biometric information.[40] Next, when moving around inside the store, beacon technology can send shoppers information, simultaneously obtaining (seemingly) innocuous information from them in return.[41] Additionally, radio frequency identification devices can track shoppers' movements around the store, analyzing the length of time a customer spends browsing, looking at a display, and general foot traffic.[42] Finally, technology implemented into the physical space has spawned the eStore's creation.[43] The eStore presents additional consumer privacy concerns, from being "helped" by an artificially intelligent interactive mirror in the dressing room to manipulating the price of an item, charging more or less for an item depending on the shopper's ability or willingness to pay.[44] Ultimately, from the shopper's entrance to their exit, physical retail stores use technology to better sell products to the shopper, often completely disregarding their privacy.

A. Facial Recognition

Facial recognition infringes upon consumer privacy when it acquires their unique individual biometric data and fails to either provide notice of this practice or provide consumers with the opportunity to opt-out of using and sharing this information.[45] Facial recognition technology, such as FaceFirst, can scan faces as far as fifty to one hundred feet away.[46] When a person walks through the

---

40 *See infra* Section II.A.

41 *See infra* Section II.B.

42 *See infra* Section II.C.

43 *See infra* Section II.D.

44 *See infra* Sections II.D.1–II.D.3.

45 There is a renewed interest in facial recognition technology, as consumer privacy groups filed a complaint with the FTC on April 6, 2018 alleging that Facebook's facial recognition technology violates the 2011 Consent Order with the FTC. *See* Complaint, In the Matter of Facebook, Inc. and Facial Recognition (filed Apr. 6, 2018); *see also* Press Release, FTC, FTC Recommends Best Practices for Companies that Use Facial Recognition Technologies (Oct. 22, 2012), https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition [https://perma.cc/KH4C-CQ6A].

46 FaceFirst, a facial-recognition software company, refuses to disclose its client list but admits that retail stores account for approximately half of the company's business. *See* Chris Burt, *FaceFirst Facial Recognition Coming to Thousands of U.S. Retail Locations*, BIOMETRICUPDATE (Aug. 21, 2018), https://www.biometricupdate.com

store's entrance, a video camera captures multiple images of the shopper, selects the clearest one, and adds their picture to the store's client database.[47] The FaceFirst software compares that image with other images in its database. If a match occurs, either recognizing the shopper as a suspected shoplifter or important client, the software can alert store employees within seconds of the person's entrance into the store.[48] After being added to the database, the software can recognize the customer on each subsequent visit to the store.[49] Similarly, retailers can pre-set pictures of individuals they wish to track in the system such as individuals suspected of burglaries based on information from nearby stores or police records.[50]

Facial recognition technology contains many potential privacy concerns because it measures and records unique biometric information. The legal issue over facial recognition primarily revolves around whether a person has the right to control who has access to his or her biometric data and how it can be used. For facial recog-

---

/201808/facefirst-facial-recognition-coming-to-thousands-of-u-s-retail-locations [https://perma.cc/3B5B-2V4E].

47 *See* David Lumb, *Is Facial Recognition The Next Privacy Battleground?*, FAST CO. (Jan. 26, 2015), http://www.fastcompany.com/3040375/is-facial-recognitionthenext-privacy-battleground [https://perma.cc/ZG57-JKA3].

48 If a designated individual is recognized, the store's facial recognition technology can alert the store that the designated person has entered the store. *See* Natasha Singer, *When No One Is Just a Face in the Crowd*, N. Y. TIMES (Feb. 1, 2014), https://www.nytimes.com/2014/02/02/technology/when-no-one-is-just-a-face-in-the-crowd.html [https://perma.cc/Z9AA-QNHN].

49 *See* Lumb, *supra* note 477.

50 *See* Singer, *supra* note 488. For example, this facial recognition technology can track a store's important customers—both the high spenders and suspicious customers. *See* Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores*, N. Y. MAG. (Oct. 20, 2018), http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html [https://perma.cc/K8PU-XS96] (recognizing that "[f]acial-recognition software, which has been in development since the 1960s . . . has taken off with retailers and event spaces during the last couple of years . . . marketed to them as an unparalleled tool for cutting down on shoplifting, and sold to the public as a security tool." While the collective and individual security risks present real dangers, the downside of it is that it is "almost completely unregulated."). This can be particularly convenient for suspicious activity or to give a high spending customer some extra assistance. *See, e.g., Face Recognition Software for Retail Stores*, FACEFIRST, https://www.facefirst.com/industry/retail-face-recognition/ [https://perma.cc/Y9NW-8665] (last visited Feb. 22, 2019).

nition technology to function properly, a company must create and maintain a database containing photos of shoppers, ever increasing with each additional new customer.[51] In addition, the typical system converts each person's face into a mathematical code, or "faceprint," extracting complex measurements of each face, which inevitably results in the use and access of another person's biometric information.[52]

Technology companies have encouraged retailers to invest and adopt facial recognition technology to better track and sell products to consumers, claiming the technology can reduce theft by more than thirty percent.[53] Moreover, retail stores using facial recognition are supposedly better able to monitor their consumers' demographic information, such as race, age, and gender, under the guise of better assisting them with more personalized options.[54]

---

[51] *See* Tabor, *supra* note 500; *see also What is Biometric Authentication?*, FACEFIRST, https://www.facefirst.com/face-recognition-glossary/what-is-biometric-authentication/ [https://perma.cc/NEN3-CBPG] (last visited Feb. 22, 2019).

[52] *See* FACEFIRST, *supra* note 511.

[53] *See* Cameron Albert-Deitch, *Your Favorite Stores Are Watching You While You're Shopping (and Collecting Your Biometric Data)*, INC. (May 2, 2017), https://www.inc.com/cameron-albert-deitch/your-favorite-stores-are-collecting-your-biometric-data-while-you-shop.html [https://perma.cc/75K3-TBRV]; *see* Phil Wahba, *Shoplifting, Worker Theft Cost Retailers $32 billion Last Year*, FORTUNE (June 24, 2015), http://fortune.com/2015/06/24/shoplifting-worker-theft-cost-retailers-32-billion-in-2014/ [https://perma.cc/REU5-2QBL] (providing statistics on "'shrinkage'—a retail-industry term which includes loss due to shoplifting, worker and vendor theft"); *see also* Leticia Miranda, *Thousands Of Stores Will Soon Use Facial Recognition, and They Won't Need Your Consent*, BUZZFEED NEWS (Aug. 17, 2018, 10:28 AM), https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at [https://perma.cc/2D8G-SZF7].

[54] Amazon Go stores embody the privacy concerns presented by facial technology, promoting it as their main feature. In Amazon Go stores, facial recognition technology "deconstruct[s] a person's facial image . . . and produces a related set of facial characteristics that the computer uses to recognize an authorized user's face." Michael Yang & Francis J. Gorman, *What's Yours is Mine, Protection and Security in a Digital World*, 36 MD. B.J. 24, 27 (2003). The relevant patents for Amazon Go stores indicate that the facial recognition software's primary use is to recognize customers. Patent US20150012396 A1 describes that "[u]pon detecting a user entering and/or passing through a transition area . . . various techniques may be used to identify a user. For example, a camera may capture an image of the user that is processed using facial recognition to identify the user." Because Amazon Go stores capture images of all customers entering their stores, Amazon can amass huge consumer information profiles, which can include hair color and skin tone. U.S. Patent No. 20150012396 A1, at [90].

In 2012, the FTC released a staff report, recommending best practices for facial recognition technology and emphasizing the importance of respecting consumer privacy.[55] The report suggested companies should obtain consumer consent before using their images or biometric data.[56] Moreover, unless the company received affirmative consumer consent, the company should not use facial recognition technology to help identify anonymous images.[57] Though the report provided meaningful recommendations, the FTC failed to require businesses to adopt these guidelines, merely suggesting best practices.[58]

However, because only Illinois and Texas have explicit laws requiring businesses to inform the public when using facial recognition technology,[59] how long they are storing it, and the third parties with whom they share these images, it remains unknown "what it takes to be put in these databases, let alone how to get [one's] name removed."[60] Additionally, because the FTC only suggested best practices for the use of facial recognition, shoppers remain overwhelmingly susceptible to infringements on their privacy.

B. Beacon Technology

Beacon technology, which transmits radio waves between communicating devices, infringes upon consumer privacy when it fails to notify consumers about their data collection, fails to obtain

---

Amazon can use this information to target specific demographic groups with advertising, to cater products in its stores to these groups, and to eliminate obsolete products.

55 *See* FTC, *supra* note 455.

56 *See id.* The use of facial recognition technology and adherence to the FTC guidelines present an obvious hurdle: obtaining consent from every person entering the store would create serious delays. Conversely, assuming individuals consent to being photographed simply because they enter the store fails to acknowledge the actual notice-and-choice guidelines, as outlined by the FTC; *see also* Daniel Keyes, *Microsoft is Developing In-Store Tracking Technology That Could Eliminate Physical Checkout*, BUS. INSIDER (June 15, 2018, 10:17 AM), https://www.businessinsider.com/microsoft-developing-in-store-tracking-technology-2018-6 [https://perma.cc/5DAU-5K5F]. Microsoft is developing technology that will track what products consumers add to their carts—charging them when they leave the store, so essentially get to leave the store without checking out. *See id.*

57 *See* FTC, *supra* note 455.

58 *See id.*

59 *See* Tabor, *supra* note 50.

60 In addition, trade secret law protects the underlying technology. *See id.*

consumer consent, and fails to inform customers how their data is used.[61] Beacon technology refers both to the underlying technology and the physical hardware of small, wireless devices that transmit Bluetooth signals to nearby devices to send and receive data. Beacon technology requires two devices to function: peripheral and secondary devices. Peripheral devices are low-powered devices that send data to the secondary device, a device such as a mobile phone, requiring greater processing capabilities.[62] Though peripheral and secondary devices can interact in a variety of ways, peripheral devices ordinarily send information and do not respond to secondary devices.[63] Because beacons are mostly limited to sending information, beacons and beacon technology are extremely affordable.[64]

Retail stores are one of the largest users of beacons.[65] For example, some retailers have embedded beacon technology into mannequins to track customers around the store.[66] After downloading a mobile application, customers can receive notifications about discounts, browse outfit ideas, and search for the availability of items.[67] In return, the retailer can obtain their information, ranging from relatively benign information, such as their age or gender, to

---

61 *See* Jules Polonetsky, *Trust, Transparency Best In-Store Deal for Shoppers with Mobile Phones*, RETAILINGTODAY (May 19, 2014), http://www.retailingtoday.com/article/trust-transparency-best-store-deal-shoppers-mobile-phones [https://perma.cc/W9LC-RBST] ("It's not a surprise that the deployment of [beacon] technologies has led to critical media stories about surprised shoppers who express annoyance when told that they are secretly having their phones tracked.").

62 Carly Huth, *A Privacy Primer on Beacon Technology*, 18 J. INTERNET L. 21 (2015).

63 Erik Vlugt, *Bluetooth Low Energy*, *Beacons and Retail,* VERIFONE, at 1, 4 (Oct. 23, 2013), http://www.verifone.es/media/3603729/bluetooth-low-energy-beacons-retail-wp.pdf [https://perma.cc/45X6-EWHA]. Further, beacons offer a range of broadcast advertising modes, including sending general advertisements that can be detected by any phone with Bluetooth functionality. *See id.*

64 *See id.*

65 *See* Huth, *supra* note 622, at 21.

66 Liat Clark, *Mannequins Are Now Digitally Tracking UK Shoppers*, WIRED UK (Aug. 12, 2014), http://www.wired.co.uk/news/archive/2014-08/12/mannequin-surveillance [https://perma.cc/4Z94-C4AR].

67 This technology allows consumers to use various discounts, while also promoting these deals to others. *See* Caitlyn Bohannon, *House of Fraser's Beacon-Enabled Mannequins Revamp In-Store Experience*, RETAIL DIVE https://www.retaildive.com/ex/mobilecommercedaily/house-of-frasers-beacon-enabled-mannequins-revamp-in-store-experience [https://perma.cc/DU8X-XASR] (last visited Feb. 22, 2019).

more insidious forms of information, such as their movements around the store.[68] In fact, some retailers are experimenting with implementation of beacon technology in smaller stores within larger department stores and smart mirrors,[69] creating countless future possibilities and applications.[70]

The privacy issues posed by beacons rest primarily in application of the technology.[71] In retail stores, beacons can send information to customers who have either enabled their Bluetooth or the corresponding retail mobile application downloaded onto their phones.[72] Beacon technology presents unique privacy concerns be-

---

[68] *See id.*

[69] A smart mirror is a two-way mirror with an electric display behind the glass, which can present the viewer with different types of information, depending on the hardware-technology included behind the glass, including internet connection, LCD display for information, etc. *See* Mauricio Ingvar, *What is a Smart Mirror?, What Can It Do for Us?*, MEDIUM (Oct. 27, 2017), https://medium.com/@Mauricio.Ingvar/what-is-a-smart-mirror-what-can-it-do-for-us-d2b762fc6878 [https://perma.cc/VPT7-D79U]; *see also* Sabrina Sandalo, *Smart Mirrors Transform Retail,* ANTEDOTE, https://antedote.com/smart-mirrors-transform-retail/ [https://perma.cc/6YBS-U7LE] (last visited Feb. 22, 2019) (describing notable examples of smart mirrors such as the Neiman Marcus MemoryMirror in San Francisco and others in Lululemon and Ralph Lauren stores in New York).

[70] *See* Bohannon, *supra* note 677 ("Lord & Taylor began partnering with brands such as Michael Kors and Alex and Ani to deliver content and offers to in-store shoppers via iBeacon technology on their smartphones when they are nearby different departments. The multi-category, multi-floor beacon deployment presents the most ambitious application of beacon marketing in the retail industry to date."); *see also* Matthew Townsend, *'Smart Mirrors' Come to the Fitting Room*, BLOOMBERG (Feb. 16, 2017), https://www.bloomberg.com/news/articles/2017-02-16/-smart-mirrors-come-to-the-fitting-room [https://perma.cc/XH8Y-E29Y].

[71] A recent update to the iBeacon's operation on the iPhone allows the technology to continue to track the user even when the application is closed. *See* Martin Kaste, *Apple Upgrade Tracks Customers Even When Marketing Apps Are Off*, NPR, (Apr. 15, 2014, 11:50 AM), https://www.npr.org/sections/alltechconsidered/2014/04/15/302990800/apple-upgrade-tracks-customers-even-when-marketing-apps-are-off [https://perma.cc/7SU8-96G9]. iBeacon is a trademarked standard for beacons from Apple. The data that iBeacon may send includes a proximity id (unique identifier) as well as other location identifiers, including specifics that could indicate the department or aisle of a store. *See* Vlugt*, supra* note 633. Androids previously had more limited functionality with respect to beacons, but this will likely change in an updated version of the operating system. *See* Molly Wood, *Businesses Are Turning to Beacons, and It's Going to Be O.K.*, N.Y. TIMES (Oct. 15, 2014), https://www.nytimes.com/2014/10/16/technology/personaltech/businesses-are-turning-to-beacons-and-its-going-to-be-ok.html [https://perma.cc/4E5E-7BXH].

[72] *See* Huth, *supra* note 622, at 21.

cause mobile applications can be designed as beneficial to the shopper's experience, which masks the *quid pro quo* relationship. Ultimately, technology that tracks consumers presents an obvious privacy issue, especially when the technology acquires sensitive personal information in the process.

C. RFID Technology

RFID technology can track both products and people within a store, with no corresponding legal doctrine guiding the use of this technology.[73] RFID tags are small electronic devices using radio frequencies to receive and transmit information.[74] Retailers use RFID technology to assist customers by locating items for purchase.[75] Additionally, retailers can use RFID to examine shopping patterns making their supply chain more efficient and improving the overall shopping experience.[76] In particular, RFID technology has provided specific advantages for fast-fashion retailers by mak-

---

[73] Eilene Zimmerman, *Bringing Digital Analytics to Main Street Retailers*, N.Y. TIMES (Aug. 27, 2014, 1:00 PM), https://boss.blogs.nytimes.com/2014/08/27/bringing-digital-analytics-to-main-street-retailers/ [https://perma.cc/GH3B-UWTY] (describing RetailNext technology).

[74] Charles J. Condon, *RFID and Privacy: A Look Where the "Chips" are Falling*, 11 APPALACHIAN J.L. 101, 102 (2011). In 2012, RFID started replacing bar codes to assist inventory management. *See id.* In addition to attaching to individual garments, RFID tags can attach to shipping materials, which allows a manufacturer to track the relevant products until they reach the destination. *See id.* RFID tags are reusable and removed from the item at checkout, helping defray costs for retailers. *See id.*

[75] Mark Hill, *How RFID Technology is Revolutionizing the Consumer Shopping Experience*, RETAIL TOUCHPOINTS (July 9, 2012), https://www.retailtouchpoints.com/features/executive-viewpoints/how-rfid-technology-is-revolutionizing-the-consumer-shopping-experience [https://perma.cc/7KB2-79VF].

[76] *See id.* For example, technologies can capture the time and location of objects in motion to quantify store performance and analyze in store anonymous customer behaviors. *See, e.g.*, Ronny Max, *People Tracking: 15 Technologies in 2018*, BEHAVIOR ANALYTICS RETAIL (Aug. 30, 2018), https://behavioranalyticsretail.com/technologies-tracking-people/ [https://perma.cc/D6K5-TXAB]; Ann-Marie Alcantara, *Adobe's Newest Labs Project Can Track In-Store Customers in Real Time,* ADWEEK (Jan. 16, 2018), https://www.adweek.com/digital/adobes-newest-labs-project-can-track-in-store-customers-in-real-time/ [https://perma.cc/V36K-7KS7] (describing the innovation project from Adobe Labs which can track live foot traffic in a store and break down shoppers into a variety of data segments).

ing items quickly available to consumers.[77] For example, more than half of Zara stores currently use RFID technology.[78]

Similarly, RFID technology can track shoppers within a store.[79] Though RFID technology generally uses a shopper's mobile phone connected to the store Wi-Fi to monitor a customer, sometimes the customer does not need to connect with the store's server to be tracked.[80] For example, in 2013, Nordstrom used Euclid Analytics

---

[77] Mass-market merchants such as Wal-Mart and J.C. Penney have adopted RFID technology into their inventory. *See* Mark Roberti, *RFID in the U.S. Retail Sector*, RFID J. (Nov. 1, 2010), https://www.rfidjournal.com/articles/view?7974 [https://perma.cc/56BE-7NGN].

[78] Prior to the use of RFID, Zara performed storewide inventories every six months, but now they perform them every six weeks, which allows Zara to create "a more accurate picture of what fashions are selling well and any styles that are languishing." The efficiency and increased speed in production helps stores like Zara because they rely on immediate production, attempting to capitalize on the latest trends. As items are sold, RFID technology immediately sends restocking orders to the stockroom for that exact item, rendering manual ordering based on written sales reports obsolete. Additionally, RFID technology allows salespeople to find products that might be sold out in that particular store but are located either at another location or online. *See* Christopher Bjork, *Zara Builds Its Business Around RFID*, WALL ST. J. (Sept. 12, 2014, 12:22 PM), https://www.wsj.com/articles/at-zara-fast-fashion-meets-smarter-inventory-1410884519 [https://perma.cc/TZB6-VTEA].

[79] MAC addresses are unique to each phone, and each address is stored to the Euclid server. *See* Sarah Perez, *Euclid, The "Google Analytics For The Real World," Partners With Aruba, Aerohive, Xirrus & Others To Make Tracking Sensor-Free*, TECHCRUNCH (Jan. 4, 2013), http://techcrunch.com/2013/01/04/euclid-the-google-analytics-for-the-real-world-partners-with-aruba-aerohive-xirrus-others-to-make-customer-trackingsensorfree/ [https://perma.cc/YPA8-YWN2].

[80] *See, e.g., Digital Mortar*, MEDIUM, https://medium.com/@Digital_Mortar [https://perma.cc/X4KY-KT57] (last visited Feb. 22, 2019) (Application which enables customer analytics for physical retail environments); *see also* Sarah Perez, *Euclid Elements Emerges From Stealth, Debts "Google Analytics For The Real World"*, TECHCRUNCH (Nov. 3, 2011), https://techcrunch.com/2011/11/03/euclid-elements-emerges-from-stealth-debuts-google-analytics-for-the-real-world/ [https://perma.cc/P488-W4XA]. However, customers have the option to opt out of the data collection on their phones, and retailers using the technology are contractually and legally obligated to make shoppers aware of the use of this technology in their stores. *See In-store Notice Guidelines*, EUCLID (Sept. 2014), https://geteuclid.com/wp-content/uploads/2015/09/euclid_instorenotice_guideline_201409.pdf [https://perma.cc/BJ9D-TGYN] (providing details on placement requirements for notices).

("Euclid") to analyze foot traffic within its retail locations.[81] Eventually, negative publicity and consumer backlash resulted in Nordstrom's decision to cease use in their stores.[82] In fact, shoppers referred to the system as "creepy" and felt that they were being stalked in the store.[83] However, Euclid could not only monitor in-store shoppers but could also monitor the number of people passing the store window, how long they may have stood there, and whether they eventually entered the store.[84] Currently, companies such as Bloomingdales, American Apparel, and Mont Blanc use RetailNext.[85] RetailNext's technology can inform the retailer how long a customer resides in each part of the store and where they might browse, using heat maps and properly distinguishing between shoppers and employees.[86] This information can identify popular products, predict when the store will be busiest, and advise the retailer on how to most efficiently organize its employees.[87]

---

81 Peter Cohan, *How Nordstrom Uses WiFi to Spy on Shoppers*, FORBES (May 9, 2013, 8:22 AM), https://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers/ [https://perma.cc/QTE3-33MX].

82 *See, e.g.*, *id.*; *see also* Euclid, *supra* note 800 ("We use Wi-Fi technology to track location analytics. This data is used to improve the store layout and enhance the customer shopping experience. The data collected is anonymous and works by sensing the presence of smartphones. No personal information is collected.").

83 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/KNA3-LB32]. Surprisingly, customers did not report these same feelings of creepiness and being stalked when shopping online, accepting that creation of online profiles and cookie collection presented similar levels of monitoring. *Id.*

84 *See* Cohan, *supra* note 811. Retailers use this information when creating window displays and when considering their overall superficial appeal to consumers. *Id.*

85 Jonathan Shieber, *RetailNext Raises Another $30 Million To Track In-Store Data*, TECHCRUNCH (July 8, 2014), http://techcrunch.com/2014/07/08/retailnext-raisesanother30-million-to-track-in-store-data/ [https://perma.cc/TE3S-UTAK].

86 *See id.; see also* Press Release, RetailNext, RetailNext 4.0 In-store Analytics Platform Now Available for Brick-and-Mortar Retailers (June 12, 2013), http://retailnext.net/press-release/retailnext-4-0-in-store-analytics-platform-now-available-for-brick-and-mortar-retailers/ [https://perma.cc/YAA9-3BE4].

87 *See* Press Release, *supra* note 866.

Though no legal doctrine governs RFID and similar tracking technologies,[88] the FTC produced four major guidelines for companies to follow when collecting data: (1) knowing what information they have and who has access to it; (2) limiting the collection and retention of information to what is necessary; (3) using secure methods to protect the information; and (4) disposing of information when its retention is no longer necessary.[89] Furthermore, the FTC concluded, "businesses deploying RFID [technology] should take steps to protect consumer privacy."[90] The FTC also indicated security measures should protect the information acquired from RFID tags.[91] This report suggested ways for businesses to respect consumer privacy and adapt practices to respect consumer concerns,[92] as the FTC expects FID technology to continue and increase in the future.[93] However, similar to other technologies, the FTC did not require businesses to adopt the report, continuing to leave shoppers vulnerable to questionable privacy practices while shopping.

D. The eStore

Due to various technologies implemented in the store, mere presence in a store presents privacy risks to customers.[94] An eStore incorporates technology into the physical retail store, automating aspects of the shopping experience while collecting data in levels

---

88 *See Radio Frequency Identification (RFID) Privacy Laws*, Nat'l Conf. of St. Leg. (Jan. 2, 2018) (indicating that only nineteen states have implemented legislation specifically addressing RFID technology).

89 *Commission Statement Marking the FTC's 50th Data Security Settlement,* FED. TRADE COMM'N, (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [https://perma.cc/U6Y9-PKFA].

90 FED. TRADE COMM'N., RFID: RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS 17 (2005).

91 *Id*. at 22.

92 *Id*. at 12.

93 *See, e.g., Services*, FACEFIRST, http://www.facefirst.com/services [https://perma.cc/ZX5N-4JDE] (last visited Feb. 22, 2019).

94 *How Stores Follow Every Step You Take*, THE ATLANTIC, https://www.theatlantic.com/sponsored/ibm-transformation/how-stores-follow-every-step-you-take/240/ [https://perma.cc/VXW7-9DLK] (last visited Feb. 22, 2019) ("Retailers have begun using location-based, context-aware advertising and marketing campaigns to attract customers to their stores. And then, once potential customers are inside, indoor location networks can take over and help them make additional sales.").

comparable to e-commerce websites.[95] Depending on the technology implemented, the eStore can predict items the shopper may want to purchase, manipulate the price, and follow-up with the shopper to remind and encourage them to purchase it.

1. The Artificially Intelligent Stylist

Increasingly, retailers use artificial intelligence to predict what shoppers might buy acting as a stylist for consumers. Artificial intelligence is "computer technology that simulates human behavior, . . . perform[ing] cognitive tasks that ordinarily require human intelligence."[96] The retail industry incorporates artificial intelligence to analyze mass quantities of data, pulling from sources such as: the individual consumer and wider market, sales figures, social media feeds, and customer product reviews.[97] Moving forward, artificial intelligence might begin further encroaching into an individual's personal information, such as their calendar appointments, and contact information for other people.[98] Brands such as Cosabella and North Face have begun experimenting with and imple-

---

[95] Bridget Johns, *The Smart Store to Become the New Face of Physical Retail*, RETAILNEXT (Oct. 5, 2016), https://retailnext.net/en/blog/the-smart-store-to-become-the-new-face-of-physical-retail/ [https://perma.cc/RA7Z-K777].

[96] Jeffrey Greene & Anne Marie Longobucco, *Is Artificial Intelligence the New Trend in Fashion?,* N. Y. L. J. (Aug. 24, 2018, 3:40 PM), https://www.law.com/newyorklawjournal/2018/08/24/artificial-intelligence-the-newest-trend-in-fashion/ [https://perma.cc/FCE8-25ZE].

[97] *See id.*

[98] *See, e.g.*, Jess Cartner-Morley, *Do Robots Dream of Prada? How Artificial Intelligence is Reprogramming Fashion*, THE GUARDIAN (Sept. 15, 2018), https://www.theguardian.com/fashion/2018/sep/15/do-robots-dream-of-prada-how-artificial-intelligence-is-reprogramming-fashion [https://perma.cc/63WX-2HWW] (discussing the ways in which MatchesFashion is experimenting with personalized digital avatars who can "wear" items being considered for purchase, and Net-a-Porter is in the testing stages of technology that can scan information such as calendar invites, future vacations, and suggest corresponding items for purchase); *see also* Ayn de Jesus*, Artificial Intelligence for Clothing and Apparel – Current Applications,* EMERJ (Feb. 16, 2019), https://www.techemergence.com/artificial-intelligence-for-clothing-and-apparel/ [https://perma.cc/SP6S-FZ49] (providing examples of start-ups that are experimenting with this recommendation technology); *see also* Daniel Faggella, *Artificial Intelligence in Retail – 10 Present and Future Use Cases,* EMERJ (Feb. 19, 2019), https://www.techemergence.com/artificial-intelligence-retail/ [https://perma.cc/F36M-RUF7] (providing examples of start-ups using recommendation technology).

menting this technology into their stores.[99] Tommy Hilfiger reportedly uses IBM's artificial intelligence technology to analyze sales performance and customer reviews for each item, even invading the design process by predicting future trends.[100]

Despite retailers' extensive use of personal data, the United States has no laws explicitly regulating artificial intelligence. However, an existing New York City law broadly calls for explanation of any decisions made via artificial intelligence.[101] By implementing artificial intelligence, retail stores attempt to personalize the consumer shopping experience but require the corresponding sacrifice of individual consumer privacy.[102]

2. Omnichannel

Retailers use omnichannel, the use of various channels to communicate with customers, blurring the line between physical and online shopping.[103] Through omnichannel, the retailer can collect information on items the consumer did not purchase and can

---

[99] *See* Cate Trotter, *The Complete Guide to AI in Retail*, INSIDER TRENDS (May 18, 2018), https://www.insider-trends.com/the-complete-guide-to-ai-in-retail/ [https://perma.cc/VR43-UH3Q].

[100] The available technology includes a color analysis tool, silhouette recognition tool and print tool, all of which allow human designers to access and combine vast numbers of images for inspiration. The software tools do the time-consuming work of analyzing trends and compiling data, allowing designers to focus on the creative process. *See id.*

[101] Dennis Garcia, *Preparing for Artificial Intelligence in the Legal Profession*, (June 7, 2017). *But see* N. Y. C., N.Y., Local Law 2018/049 (2018).

[102] *See* Greene & Longobucco, *supra* note 966.

[103] BIGCOMMERCE, 2018 OMNICHANNEL BUYING REPORT 7 (2018); *see also* Peter C. Verhoef et al., *From Multi-Channel Retailing to OmniChannel Retailing Introduction to the Special Issue on Multi-Channel Retailing*, 91 J. OF RETAILING 174, 174 (2015) (asserting that retailers must decide "as to whether new channels should be added to the existing channel mix. This decision pertains to traditional brick-and-mortar players, as well as to new online players, who face the question of whether they should be present offline as well."); *see also* Hemant K. Bhargava et al., *The Move to Smart Mobile and its Implications for Antitrust Analysis of Online Markets*, 16 U.C. DAVIS BUS. L. REV. 157, 172 (2016) ("These changes in consumer shopping behavior are resulting in a revolution in retail. Retail stores are developing 'omnichannel' approaches that integrate physical stores, mobile apps, and websites to provide consumers with multiple choices of how to shop and buy.").

send follow-up messages to remind the shopper about the item under the guise of inquiring about their interest.[104]

This blurring of online and physical shopping has incentivized retailers to create a seamless overall shopping experience. Notable retailers including Amazon, Walmart, and Zara have already implemented omnichannel shopping into their stores.[105] Other retailers, such as Sephora, have implemented programs to inform the customer about products that similar like-minded consumers have supposedly purchased. In fact, Sephora's Beauty Boards portray uploaded photos of customers using their products, allowing shoppers to look at the images and decide which products they may want to buy.[106] Moreover, through its "My Beauty Bag" program, customers can easily toggle between their interested products, purchase items in store and online, re-order items, manage all purchase orders, and track purchases.[107]

Similarly, through an eBay partnership, Rebecca Minkoff created the "Connected Store," presenting an omnichannel shopping experience through a variety of platforms in its San Francisco and New York stores.[108] At the point of entry, the customer connects to

---

[104] Lauryn Chamberlain, *Rebecca Minkoff And The 'Store Of The Future'*, GEOMARKETING (Jan. 18, 2017, 2:03 PM), https://geomarketing.com/rebecca-minkoff-and-the-store-of-the-future [https://perma.cc/QJ9W-QR6S]; *see also* Daniel Faggella, *Three AI Marketing Trends for Brick-and-Mortar Retailers*, MARTECH (May 3, 2018, 4:24 PM), https://martechtoday.com/three-ai-marketing-trends-for-brick-and-mortar-retailers-214917 [https://perma.cc/C6M8-AFU4] (identifying three trends: (1) anticipating customers' needs, (2) driving customers back to the store or delivering to them, and (3) out of store recommendations and advertising).

[105] *See Zara Opens a High-Tech Omnichannel Store*, BLOOMBERG (May 18, 2018), https://www.digitalcommerce360.com/2018/05/18/zaras-high-tech-omnichannel-store/ [https://perma.cc/J2DA-X5K4]; Tommy Walker, *Omni-Channel Retailing: What Is Omni-Channel Commerce, Really?*, SHOPIFY (Jan. 29, 2018), https://www.shopify.com/enterprise/omni-channel-retailing-commerce-what#What's-Next-for-Omni-Channel-Retailing? [https://perma.cc/R6B3-SZDM].

[106] Jason Trout, *5 Excellent Examples of Omnichannel Retailing Done Right*, MULTICHANNEL MERCH. (Feb. 2, 2017), https://multichannelmerchant.com/must-reads/5-excellent-examples-omnichannel-retailing-done-right/ [https://perma.cc/J9AZ-3KLX].

[107] *Id.*

[108] Chamberlain, *supra* note 1044; Caitlyn Bohannon, *Rebecca Minkoff Tosses Cash Registers with New Connected Store*, RETAILDIVE (Feb. 2, 2017), https://www.retaildive.com/ex/mobilecommercedaily/rebecca-minkoff-tosses-cash-registers-with-new-soho-connected-store [https://perma.cc/Y9Z3-3PVW]; Allie

the store through their smartphone.[109] A large touchscreen then greets customers at the entrance, allowing them to browse through the store's inventory and request pieces to be sent to a dressing room.[110] When ready, the shopper can be alerted via cell phone.[111] In the dressing room, the RFID shields detect the clothing,[112] with its mirrors functioning as touchscreens, which can allow the customer to customize the dressing room lighting, and request additional items.[113] When done trying on clothing, the customer can complete the transaction on a sales associates' iPad, with the option of using their loyalty cards to complete the purchase, as no traditional registers appear inside the store.[114] Overall, the entire shopping experience is perfectly seamless: digital, personalized, and convenient. After implementation of its "connected store," Rebecca Minkoff reported a tripling in its clothing sales.[115]

Similar to artificial intelligence, no existing legal doctrine governs omnichannel shopping because omnichannel shopping combines multiple technologies into a single concept.[116] However, omnichannel shopping in the physical retail space world is a growing reality.[117] Though the American legal system cannot yet address

---

Abodeely, *The Future of Omni-Channel: Insights, Innovations & Experiences*, COLUM. BUS. SCHOOL (June 17, 2015), https://www8.gsb.columbia.edu/articles/brand-talk/future-omni-channel-insights-innovations-experiences [https://perma.cc/U8EU-WCN7].

109 *See* Chamberlain, *supra* note 1044; *see also* Bohannon, *supra* note 67.

110 *See* Chamberlain, *supra* note 1044.

111 *See id.*

112 *See id.*

113 *See id.*

114 Ava Farshidi, *The New Retail Experience and Its Unaddressed Privacy Concerns: How RFID and Mobile Location Analytics are Collecting Consumer Information*, 7 CASE W. RESERVE J. L. TECH. & INTERNET 15, 23 (2016).

115 Hilary Milness, *How Tech in Rebecca Minkoff's Fitting Rooms Tripled Expected Clothing Sales*, DIGIDAY (Sept. 23, 2015) https://digiday.com/marketing/rebecca-minkoff-digital-store/ [https://perma.cc/H7V3-SVZD]. For example, thirty percent of customers requested additional items to be sent to the dressing room using the smart mirror touch screen.

116 *But see* EUROCOMMERCE, E-COMMERCE, OMNI-CHANNEL RETAIL, AND EU POLICY 8 (2014).

117 *Omnichannel Fast Facts On The In-Store And E-Commerce Landscapes,* NIELSEN (Oct. 18, 2018), https://www.nielsen.com/us/en/insights/news/2018/omnichannel-fast-facts-on-the-in-store-and-e-commerce-landscapes.html [https://perma.cc/L6P7-JDNR]; Jean-Marc Bellaïche, *The Omnichannel Opportunity for Retailers*, BOSTON CONSULTING

omnichannel shopping, it must act soon, considering the significant privacy implications.

3. Dynamic Pricing

By using multiple tracking technologies, retailers can manipulate the availability, cost, and appeal of an item.[118] Dynamic pricing uses existing customer information to determine the ideal cost at which a shopper will purchase a particular product.[119] Consumers provide retailers with this information "whenever they make a credit card purchase[,] . . . use free e-mail services, surf [the Internet] for information[,] or engage in social media."[120] As a result, retailers can inflate the price to consumers willing and able to pay more, while offering the same product to other consumers for less money.[121]

Moreover, retailers can purchase the data obtained by social media platforms, such as shoppers' e-mail addresses and other personal information.[122] For example, social media platforms such as Facebook, Twitter, and Instagram use first-party cookies. Howev-

---

GRP. (July 18, 2013), https://www.bcg.com/en-us/publications/2013/marketing-sales-omnichannel-opportunity-retailers.aspx [https://perma.cc/GD3V-NPXG].

118 Stephanie Pandolph, *Shoppers Expect More Personalization*, BUS. INSIDER (Oct. 26, 2017, 11:13 AM), https://www.businessinsider.com/shoppers-expect-more-personalization-2017-10 [https://perma.cc/TPW4-PN53]; Victoria Greene, *7 Examples of Big Data Personalization*, BIG DATA (Oct. 11, 2018), https://bigdata-madesimple.com/7-examples-of-big-data-retail-personalization/ [https://perma.cc/F83J-ZEHL].

119 Paul Krugman, *Reckonings; What Price Fairness?*, N.Y. TIMES (Oct. 4, 2000), http://www.nytimes.com/2000/10/04/opinion/reckonings-what-price-fairness.html [https://perma.cc/TZ2U-4XRN]. Dynamic pricing uses consumers' "electronic footprint[s]"—their record of previous purchases, their addresses, and maybe other sites they have visited. *Id.*

120 Akiva A. Miller, *What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing*, 19 J. TECH. L. & POL'Y 43, 91 (2014).

121 *See* Krugman, *supra* note 11919. Amazon and other companies are reluctant to discuss information regarding their e-commerce practices because of the negative publicity associated with differential pricing. Adam Tanner, *Different Customers, Different Prices, Thanks to Big Data*, FORBES (Apr. 14, 2014), https://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/#2dc306a75730 [https://perma.cc/UMR2-FU7S].

122 *See* Robert M. Weiss & Ajay K. Mehortra, *Online Dynamic Pricing: Efficiency, Equity and the Future of E-Commerce*, 6 VA. J.L. & TECH. 11 (2001) (discussing dynamic pricing and its resulting impact on consumers).

er, technologists have created a "super" or "Flash" cookie, which is embedded into web pages and always stored outside of the browser's control.[123] Unfortunately, these same "[w]eb browsers do not directly allow users to view or delete the cookies stored by a Flash app, [and] users are not notified when such cookies are set, and these cookies never expire."[124] Therefore, when users clear their cookies, super or Flash cookies allow a website to "respawn" the information stored from the deleted cookies, effectively retaining all collected information and circumventing traditional cookie policies.[125] In other words, super and Flash cookies can "rebuild a user's information profile even after the user has erased [their] cookie history."[126] Ultimately, this technology allows companies to target new consumers that might be interested in their products.[127]

Retailers can contract with social media platforms and other applications using enhanced cookies to create new consumer targets.[128] This information enables retailers "to develop a broad picture about a consumer, such as identifying that the individual owns a house, runs marathons, eats healthy food, has a premium bank card, and is good in financial health."[129] This information, mostly collected without consumers' knowledge or consent, allows retailers to charge individuals more or less money. Overall, retailers with a social media presence take advantage of this collected information to further maximize profits.

In addition to antitrust laws, consumers have attempted to use criminal law to address price discrimination, which eventually failed.[130] Case law indicates retailers can differentiate prices when

---

123 Heather Traeger & Kris Easter, *Use of Social Media in Private Fund Offerings: Perks, Perils, and Privacy*, 13 J. BUS. & SEC. L. 143, 147 (2007).

124 Seth Schoen, *New Cookie Technologies: Harder to See and Remove, Widely Used to Track You*, ELEC. FRONTIER FOUND. (Sept. 14, 2009), https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide [https://perma.cc/67R7-FDQ2].

125 *Id.*

126 *Id.*

127 Traeger & Easter, *supra* note 1233, at 147.

128 *Id.*

129 *Id.*

130 Katzman v. Victoria's Secret Catalogue et al., 167 F.R.D. 649, 661 (S.D.N.Y. 1996); Katzman v. Victoria's Secret Catalogue, No. 96-7929, 113 F.3d 1229, *1 (2d. Cir. 1997).

based on reasonable business practices, such as customer reward programs, only outlawing price discrimination when using race, gender, or other suspect class.[131] Though the FTC has not yet regulated dynamic pricing, the FTC might re-examine whether it presents an "unfair" business practice based on its use of developing technology to extract a consumer's information.[132] In its 2014 guidance, the FTC seemingly recognized that it would eventually involve itself in this murky legal area in the future.[133]

III. THE LAW LAGS BEHIND TECHNOLOGICAL ADVANCEMENTS WITH NO AVAILABLE JUDICIAL RECOURSE

The myriad of privacy issues presented by retail stores' implementation of technology can be distilled into one overarching problem: retail stores fail to adequately consider consumer privacy when implementing new technologies. Advanced technologies present unique challenges for judges, lawmakers, and agency regulators because they must apply outdated legislation to contemporary technologies.[134] Unfortunately, the existing privacy torts cannot

---

131 Weiss & Mehrota, *supra* note 1222, at 28.

132 *Id.* at 34; Marisa Schultz, *Schumer: Airlines Want to 'Big Brother' Your Fares*, N.Y. POST (Mar. 11, 2018, 5:16 PM), https://nypost.com/2018/03/11/schumer-calls-for-ftc-to-investigate-dynamic-pricing-by-airlines/ [https://perma.cc/T8KA-93PR].

133 Guides for Advertising Allowances and Other Merchandising Payments and Services, 79 Fed. Reg. 58,245 (Sept. 29, 2014) (to be codified at 16 C.F.R. pt. 240), https://www.ftc.gov/system/files/documents/federal_register_notices /2014/09/140929fredmeyerfrn.pdf [https://perma.cc/T264-UTP5]; Anthony V. Lupo et al*., Incentives and Promotions in the Fashion Arena: The FTC Weighs In*, FASHION L. BLOG (Dec. 15, 2014), https://s3.amazonaws.com/documents.lexology.com/5786130d-ab9d-4aeb-b0f6-429576afde1d.pdf [https://perma.cc/XXB7-H35Y].

134 Paul Dughi*, Facebook: Tracking Your In-Store Visits and Serving Ads?*, MEDIUM (Aug. 13, 2017), https://medium.com/social-media-growth-hacking-hub/facebook-tracking-your-in-store-visits-and-serving-ads-af592fb0a890 [https://perma.cc/54FA-Z96W] (describing a developing practice of advertisers targeting shoppers online after the shopper has visited the physical store). This cross-promotional advertising necessarily implicates a variety of laws considering it involves a variety of actions and locations. *See id.* Thus, the question remains: when asked to rule on its legality, how will a judge decide? *See id.* Evaluating its legality on a purely physical or virtual level is incomplete, and the legal landscape has not confronted the question of how to decide the legality of a practice that is simultaneously online and virtual. *See id.*; *see also* Morgan Hochheiser, *The Truth Behind Data Collection and Analysis*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 32, 33 (2015). For example, Target specifically collected data on

adequately address the privacy issues presented by brick-and-mortar stores. In addition, the FTC remains underequipped. As a result, shoppers are left with no legal recourse.

Claims relying on the privacy torts fail.[135] The current judicial conceptualization of privacy law has foreclosed the application of the privacy torts against retail stores. Courts continue to rely upon antiquated and narrow understandings of privacy, finding it non-existent if the information has either been exposed to the public or disclosed to others.[136] In short, developing technology has outpaced the privacy torts.[137]

Of the four privacy torts, intrusion upon seclusion could theoretically apply to retail stores, but no successful claim has been litigated.[138] A successful intrusion upon seclusion claim requires an intrusion into a person's private matters that is highly offensive to a reasonable person.[139] Therefore, physical presence in the store prevents this tort's applicability because the shopper has "willingly" albeit necessarily appeared in public. In addition, intrusion upon seclusion only protects acts "highly offensive" to a reasonable person.[140] Much of the information gathered, used, and disseminated by retailers occurs periodically, often involving relatively innocuous information that fails to satisfy the threshold required.[141]

---

pregnant women that shopped in its stores, gave it to a third party to analyze, and began offering these women personalized coupons. One teenage girl's father was notified of her pregnancy when the coupons arrived at their home. The story gained national attention and raised major privacy concerns among consumers about the quantity of personal data Target was collecting. *Id.* at 32–33.

135 *See* Clark D. Asay*, Consumer Information Privacy and the Problem(s) of Third-Party Disclosures,* 11 NW. J. TECH. & INTELL. PROP. 321, 330 (2013); Neil M. Richards*, The Limits of Tort Privacy,* 9 J. ON TELECOMM. & HIGH TECH L. 357, 359 (2011); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1805 (2010); Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 1054 (1995).

136 *See id.* at 1920.

137 *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1918 (2010) (describing the inherent limitations of the privacy torts).

138 *See* RESTATEMENT (SECOND) OF TORTS § 652B (Am. Law. Inst. 1979).

139 *Id.*

140 *See id.*

141 *See* Shibley v. Time, Inc., 341 N.E. 2d 337, 339–40 (Ohio Ct. App. 1975) (finding that "selling subscription lists to direct-mail advertisers" is not sufficient to give rise to an

Finally, attempted intrusion upon seclusion claims fail because courts usually require an intrusion into the person's home or alternative place of seclusion, unwilling to extend this tort's applicability to public spaces.[142]

Furthermore, courts have rejected appropriation of one's name or likeness as a possible tort for consumers to protest the sale of their personal information. The tort of appropriation requires appropriation of another's name or likeness for personal gain, foreclosing the possibility of addressing the collection, use, and dissemination of personal data.[143] To succeed, the plaintiff must show that the "[d]efendant, without permission, has used some aspect of identity or persona in such a way that plaintiff is identifiable from defendant's use" and that the "[d]efendant's use is likely to cause damage to the commercial value of that persona."[144]

In *Dwyer v. American Express Co.*, the court found the defendant credit card company was not liable when it sold its cardholders' names to third party merchants because "an individual name has value only when it is associated with one of defendant's lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendant's practices do not deprive any of the cardholders of any value their individual names may possess."[145] *Dwyer* indicates that the appropriation privacy tort does not apply to retail stores because shoppers are not deprived of any monetary value if they are photographed entering the store or if their information is compiled and sold. Because this tort focuses solely on commercial exploitation, it does not apply to the average

---

action for intrusion). Retailers similarly obtain seemingly innocuous pieces of information about their customers, including age, financial status, time spent shopping, previous purchases, etc. If analyzed under the same standard, courts likely would not consider these retail practices to be invasions of privacy.

142 *See* RESTATEMENT (SECOND) OF TORTS § 652B (Am. Law. Inst. 1979). The right to privacy does not allow individuals to prevent a particular disclosure from being made. Rather, it provides an actionable tort that may be brought by the aggrieved victim of a violation of the right to privacy. *See id.*

143 *See* RESTATEMENT (SECOND) OF TORTS § 652C (Am. Law. Inst. 1979).

144 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 3:2 (2d ed. 2004) (citations omitted).

145 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995).

shopper in a retail store.[146] Because a successful claim requires the use of an identity that is commercially valuable, the average person whose images enter searchable databases will not be saved by a successful misappropriation claim.[147]

The remaining two privacy torts, false light and public disclosure of private facts seemingly do not apply to the technologies implemented in retail stores.[148]

IV. HOW INCREASED FTC REGULATION CAN PREVENT RETAIL STORES FROM INVADING SHOPPER'S PRIVACY

Until the courts become available, aggrieved individuals must rely on the FTC to protect their privacy interests. As such, the FTC must increase its policing of retail store technologies because FTC decisions are the functional equivalent of common law.[149] When analyzing previous decisions, the FTC appears willing to defend consumer privacy in physical retail stores.[150]

---

[146] *See* Melville B. Nimmer, *The Right of Publicity*, 19 LAW AND CONTEMPORARY PROBLEMS 203, 204 (1954).

[147] *See* Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 895 (2006). A possible plaintiff who could allege a successful appropriation claim against a retail store might be a celebrity; a theoretical proposition outside the scope of this Article.

[148] Public disclosure of private facts creates a cause of action when one makes public through widespread disclosure "a matter concerning the private life of another" in a way that "(a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." RESTATEMENT (SECOND) OF TORTS § 652D (Am. Law. Inst. 1979). Because many uses of data by companies do not involve widespread disclosure and do not involve data that would be highly offensive if disclosed, the tort proved to be of little use. As a result, few cases involving the privacy torts were brought in situations involving problems with the collection and use of personal data. Similarly, the false light tort creates a cause of action when one who gives publicity to another that places the other before the public in a false light if the false light in which the other was placed would be highly offensive to a reasonable person and the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed. RESTATEMENT (SECOND) OF TORTS § 652E (Am. Law. Inst. 1979).

[149] *See* Solove & Hartzog, *supra* note 15, at 606–27 (analogizing FTC settlements to de facto common law).

[150] Thomas C. Bell, et al., *FTC Ramps Up Scrutiny of Retail Location Analytics*, PERKINS COIE (May 8, 2015), https://www.perkinscoie.com/en/news-insights/ftc-ramps-up-scrutiny-of-retail-location-analytics.html [https://perma.cc/J6NM-

If the FTC increases its policing of retail stores, the FTC first appears likely to require prominent signage to inform potential customers that tracking and monitoring occurs within the store. Second, the FTC would likely require explicit customer consent to use of the technology. Third, considering its disapproval of targeted advertising based on a shopper's precise location, the FTC would likely impose limitations on tracking technology. Finally, the FTC would likely limit the retailer's collection and use of their customers' personal information for targeted advertising.

A. Prominent Notice

If the FTC increases its policing of physical retail stores, the FTC would likely require prominent signage informing entering customers that tracking occurs within the store. In a previous decision, *In re Nomi Techs., Inc.*, the FTC penalized the company for its failure to display the required information.[151] The original complaint alleged Nomi began marketing its "Listen" technology in retail stores to better understand customer traffic.[152] The FTC indicated Nomi deceived customers because (1) its privacy policy stated customers could opt-out at retail stores when retail stores implemented no mechanism to opt-out, and (2) Nomi's privacy policy implied Nomi would notify customers about its data collection practices so customers would be informed and could opt-out.[153]

Nomi collected this customer traffic information to provide analytics for its clients.[154] Nomi provided information including: the number of customers entering the store, the time spent shopping inside the store, and whether customers visited other store loca-

---

XNJG] ("Together these developments serve as a reminder to analytics firms and to the retail, hotel and other clients they serve that the FTC is watching, and businesses must live up to the privacy promises made in connection with these forms of tracking technologies."); *see also* Ashkan Soltani, *Privacy Trade-Offs in Retail Tracking*, 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/7B2F-6AP2].

151 *See, e.g.*, Decision and Order at 2, *In re* Nomi Techs., Inc. (No. C-4538), 2015 WL 5304114 (FTC Aug. 28, 2015) (ordering Nomi not to "misrepresent in any manner" customers' notice and choices).

152 *Id.* at 1–2.

153 *Id*. at 2.

154 *Id.* at 1–2.

tions.[155] Because the retail stores failed to notify customers of their use of Nomi's technology,[156] customers remained unaware that they were being tracked while shopping in the store.[157] In other words, notice was completely absent, except in an online privacy policy that few consumers would even think to consult. As a result, the FTC indicated companies should comprehensively describe how they would share and use their customers' information by notifying the consumer.[158]

B. Opt-In Consent

If it increased its enforcement actions with retail stores, the FTC would likely require customer consent before physical retail stores could collect their information. On February 6, 2017, the FTC issued a complaint against VIZIO, Inc., ("VIZIO") a manufacturer of Smart TVs.[159] The complaint simultaneously applied the FTC's Section 5 unfairness authority while proposing a new "unfair tracking" standard.[160] The FTC alleged that VIZIO, without obtaining consent, collected and shared individual viewing data with third parties.[161] As a result of the subsequent settlement, VIZIO agreed to a new set of notice-and-choice rules for the collection and use of their customers' information.[162]

The final FTC order established a new set of notice-and-choice rules for the collection of data: (1) before collection, the consumer must receive notice, which must appear "separate and apart" from a privacy policy or terms of service and must be unavoidably

---

155 *Id.*

156 *Id.*

157 *Id.* However, Nomi did have an online privacy policy, through which a hypothetical consumer might have read that she could opt-out of the data collection either online or at the retail stores where the data collection was enabled. *Id.* at 2–3. The online privacy policy was not required to be seen or consented to by a shopper, and a shopper would have to know on their own which retailers used the technology and where to find the policy. *Id.* at 2.

158 *VIZIO* Stipulated Order, No. 2:17-cv-00758 4 (D.N.J. Feb. 6, 2017).

159 Complaint at ¶ 1–2, 4, FTC v. VIZIO, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017).

160 *Id.* at ¶ 35.

161 *Id.* at ¶ 33.

162 *VIZIO* Stipulated Order, *supra* note 15858, at 4.

"prominent";[163] (2) the notice must contain specified substantive elements, including which types of data will be collected, what will be shared with third parties, and the reason for sharing that data;[164] and (3), when notice is provided, the consumer must provide authentic "opt-in" consent before any data is collected.[165]

Additionally, the final order created a new "unfair tracking" standard to be applied to a new category of "sensitive" information. This settlement indicates the FTC's willingness to broadly interpret the unfairness standard to establish new rules and enforcement tools. Though the claim was eventually settled, the FTC indicated previously accepted passive methods of obtaining consent to a privacy policy or terms of service would be more heavily scrutinized moving forward.[166]

C. Precise Location

Based on the FTC's complaint against InMobi, the FTC appears wary of technologies that track consumers' precise locations..[167] InMobi created a software development kit ("SDK") that could be used by mobile applications to push advertisements to the user.[168] In other words, mobile application developers could integrate SDK technology into their respective application, which would deliver advertisements to the user, ultimately making it more financially attractive.[169]

---

163 *Id.*

164 *Id.*

165 *Id.* This third component of the final FTC order is important because the burden switches from an opt-out on the part of the consumer to an opt-in. *See* Alan McQuinn, *The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules*, INFO. TECH. & INNOVATION FOUND. (Oct. 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules [https://perma.cc/QZ5E-9GXS].

166 *See e.g.*, Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA HIGH TECH. L.J. 483 (2015); Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369 (2017).

167 Complaint at 13–14, United States. v. InMobi Pte Ltd., Case No.: 3:16-cv-3474, (N.D. Cal. 2016).

168 *Id.* at 3.

169 *Id.*

The InMobi SDK technology allowed advertisers to target consumers based on their geographic locations.[170] When a user installed a mobile application using InMobi SDK technology, users were prompted to grant the application access to their location.[171] Unless disabled, the InMobi SDK would select advertisements based on their location, and begin pushing these advertisements to the user.[172]

Throughout this process, the InMobi SDK also collected data about the device's Wi-Fi network.[173] Unless disabled, InMobi collected the device location along with details about the Wi-Fi network to which it was connected at the time.[174] With this information, InMobi could identify the user's precise location.[175] As a result, InMobi targeted advertisements to users based on their exact location, identifying their whereabouts without notice or consent.[176] The FTC alleged InMobi deceived developers who incorporated the InMobi SDK into their mobile application, in addition to the obvious deception to the individual actually using the application, indicating its disapproval of the use of technologies to track individuals' locations.[177]

D. Collection of Personal Information

In emphasizing the importance of limits for tracking and obtaining consumer consent, the FTC seems to disapprove of companies' routine collection of personal data.[178] In a previous enforcement action against Sears, the FTC issued a complaint alleging Sears failed to disclose how much personal information it collected

---

170 *Id.* at 3–4.

171 *Id.* at 5. However, if the user chose to disable access to the device's geo-location, the mobile device would not make the data available to inMobi. *Id*.

172 *Id.* at 4.

173 *Id.* at 5.

174 *Id.* at 6.

175 *Id.*

176 *Id.*

177 *Id.* at 9.

178 *In the matter of Sears Holding Mgmt. Corp.,* 4264 F.T.C. 0823099, at 5 (2009); Press Release, FTC, Sears Settles FTC Charges Regarding Tracking Software (June 4, 2009), https://www.ftc.gov/news-events/press-releases/2009/06/sears-settles-ftc-charges-regarding-tracking-software [https://perma.cc/GR9W-U4YB] [hereinafter FTC Sears].

from consumers after they had downloaded the software.[179] Sears advertised its software to customers indicating it would provide greater opportunities for discounts by tracking their internet history.[180] However, Sears collected additional information, which included "the contents of shopping carts, online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for web-based e-mails."[181]

The software effectively tracked all personal information consumers had available on their computers, without obtaining their consent.[182] Sears eventually settled with the FTC and agreed to destroy all the amassed consumer personal information.[183] Based on this agreement, it came as a surprise that the Federal Trade Commission approved a petition by Sears Holding Management requesting that the FTC reopen and modify this same 2009 FTC order after a public comment period.[184]

---

179 *See generally In the matter of Sears Holding Mgmt. Corp.,* 4264 F.T.C. 0823099, at 5 (2009).

180 *Id.*

181 *Id.* at 5.

182 *Id.* at 2. The FTC's previous enforcement action against Sears compares to the technology currently being implemented in Amazon Go stores, where just by walking into the store, consumers will have their every move tracked, picture taken and stored, and personal information and shopping patterns stored in the Amazon Go system without consenting. *See* Amazon Go, *Frequently Asked Questions*, https://www.amazon.com/b?node=16008589011 [https://perma.cc/9SM2-RW4Y] (last visited Feb. 22, 2019). As a result, the language of Section 5 must be amended so the FTC can provide guidance and restrictions on the technology implemented into Amazon Go physical stores. *See id.*

183 FTC Sears, *supra* note 17878. A Sears' representative stated that in the future if it "advertises or disseminates any tracking software in the future, it will clearly and prominently disclose the types of data the software will monitor, record, or transmit." *Id.* Sears fulfilled this agreement by disclosing on a separate screen from the privacy policy and license agreement: (1) all of the types of data that the Tracking software would monitor, record, or transmit, (2) how the data would be used, and (3) whether the data would be used by a third party. *Id.* It was beneficial to consumers that the FTC stepped in to make sure personal information outside the scope of its tracking policy was destroyed and that the company became more transparent. *Id.*

184 *Id.*

E. Targeted Advertising

Finally, the FTC appears to disapprove of targeted advertising, as it may constitute a deceptive practice. *In Turn, Inc.,* the FTC addressed a matter of "tracking" and targeted advertising.[185] The company offered a digital marketing platform ("DMP"), which allowed advertisers to target consumers across multiple devices.[186] To personalize the targeted advertising, Turn combined user activity on the Internet with the information obtained across devices.[187]

Some Internet users routinely clear their Internet history to avoid identification, resetting their device advertising identifiers.[188] However, Turn circumvented this avoidance by collecting an identifier called a Unique Identifier Header ("UIHD") from its Verizon Wireless Network users.[189] As a result, even if Verizon users deleted their Internet history, Turn could still identify and send advertisements to them because of the UIHD.[190] According to the complaint, Turn posted privacy guidelines, which incorrectly stated users could opt-out of this tracking.[191] The FTC identified this statement was deceptive because it excluded Verizon users.[192] Ultimately, Turn agreed to a settlement order with the FTC.[193]

As a result of this action, the FTC recently adopted a theory of "unfair tracking," creating a new tool to regulate businesses and new technology in future privacy cases. Furthermore, VIZIO created new notice and opt-in consent requirements for the purposes of sensitive "viewing data."[194] Retail stores that collect and use consumer data should consider this decision when implementing or continuing their own collection practices.

---

185 Complaint at ¶¶ 16–19, *In the matter of Turn Inc.,* 4612 F.T.C. 1523099 (2017).

186 *Id.* at ¶¶ 3. This specific targeting appears almost as an extension of the omnichannel shopping experience, with relevant characteristics from beacon and RFID technology. *See supra* Part III.

187 Complaint at ¶ 5, *In the matter of Turn Inc.,* 4612 F.T.C. 1523099 (2017).

188 *Id.* at ¶ 7.

189 *Id.* at ¶ 8.

190 *Id.* at ¶¶ 9–10.

191 *Id.* at ¶¶ 11–14.

192 *Id.* at ¶¶ 16–20.

193 Agreement Containing Consent Order, Turn Inc., No. 152-3099, 2016 WL 7448417 (FTC Dec. 20, 2016).

194 *VIZIO* Complaint, *supra* note 15959, at ¶ 33.

CONCLUSION

While advances in technology can benefit traditional retailers and consumers, legal safeguards must be enforced to protect individual privacy. Currently, the rate of technological advances and the delayed legislative response have created a disregard for individual privacy. As the de facto American privacy regulator, the FTC must be empowered to regulate the physical retail space, requiring increased resources and enforcement tools. Until the American legal system reconsiders its misguided conceptualization of privacy, the FTC remains the only entity able to protect shoppers within the physical retail space.