THE NEW RETAIL EXPERIENCE AND ITS UNADDRESSED PRIVACY CONCERNS: HOW RFID AND MOBILE LOCATION ANALYTICS ARE COLLECTING CUSTOMER INFORMATION

Ava Farshidi

INTRODUCTION

Americans love to shop. Shoppers can shop in any platform, at any time, and anywhere to get just about anything they want. The fashion industry has been at the forefront of customizing the customer experience,[1] and the emergence of omnichannel has shown the significance of connecting brick and mortar stores with digital means of shopping through the Internet and mobile apps.[2] The result of increased technology to facilitate the shopping experience requires the collection of data. Where there is collection of data, there are privacy concerns to be addressed. Pam Dixon, the executive director of the World Privacy Forum, has remarked that the media has focused on companies' tracking through Internet browsers, but the public is, for the most part, unaware of how brick and mortar stores are tracking them.[3] She comments, "This is an entire business model that has sprung up that I think maybe three people in the entire country know about outside the industry."[4] Some of the technology that fashion retailers are now using is so foreign to legal regulators that the privacy implications have not yet been clearly confronted. Throughout the shopping evolution we have gone from brick and mortar to online to eStore—the latest shift in the shopping experience merging technology and the brick and mortar space.

1. Lauren Sherman, *A Customized Experience for Each Shopper?* BUSINESS OF FASHION (Dec. 8,2014), http://www.businessoffashion.com/articles/fashion-tech/customised-experience-shopper.
2. Daniel Newman, *The Omni-Channel Experience: Marketing Meets Ubiquity*, FORBES July 22, 2014, http://www.forbes.com/sites/danielnewman/2014/07/22/the-omni-channel-experience- marketing-meets-ubiquity/. ("Marketers now need to provide a seamless experience, regardless of channel or device. Consumers can now engage with a company in a physical sore, or an online website or mobile app, through a catalog, or through social media. They can access products and services by calling a company on the phone, by using an app on heir mobile smartphone, or with a tablet, a laptop, or a desktop computer. Each piece of the consumer's experience should be consistence and complementary.").
3. Christopher Matthews, *Private Eyes: Are Retailer Watching Our Every Move?* TIME (Sept. 18, 2012), http://business.time.com/2012/09/18/private-eyes-are-retailers-watching-our-every-move/.
4 *Id*.

Part I of this paper will look at the newest development of the retail experience and suggest a method to understand the privacy concerns as well as suggest a regulatory scheme to protect customers without inhibiting their shopping experience. Part II will provide a background of the three stages of shopping experiences and the evolution of privacy concerns associated with them. Part III will address the current American stance on data collection and privacy law with a particular look at privacy concerns that the eStore is facing. Finally, Part IV will provide guidance on how to deal with these data collection issues in the future and attempt to answer two questions:

(i) Does the definition of data collection need to be adjusted? and (ii) Are customers ready to accept the new eStore?

I. BACKGROUND

A. American Consumers Have Always Associated Brick and Mortar Stores as Limited in their Data Collection, While they Have Remained Cautious in their Online Shopping.

Jerry Kang ("Kang") pinpoints the comparison between a customer's experience in a mall in both real space and in cyberspace.[5] Analyzing the customer in a mall in real space, the customer experiences relative anonymity- the only people who are tracking the customer as the customer walks through the mall, browses the store, and makes a final purchase are the other people in the same real space.[6] Other than overeager sales associates, it is unlikely anyone will remember what the customer chose, how long the customer was in the store, and how long the customer held that navy leather handbag. The greatest data concern the customer will have is at the point-of-sale if the customer chooses to pay with a debit or credit card, which is "detailed, computer-processable, indexed by name, and potentially permanent."[7]

Shift the perspective of the customer in the mall to cyberspace, where the amount of information collected about the shopper mirrors the amount that is not collected in the brick and mortar store.[8] Retailer websites collect information about every item looked at, what is ordered, and the time spent on the website.[9] All this detailed and permanent information also includes

5. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1198 (1998).
6. *Id.*
7. *Id.*
8. *Id.* ("By contrast, in cyberspace, the exception becomes the norm: Every interaction is like the credit card purchase.").
9. *Id.* at 19 ("As soon as you enter the cyber-mall's domain, the mall begins to track you through invisible scanners focused on your bar code. It automatically records which stores you visit, which windows you browse, in which order, and for how long.").

personal credit or debit card information, as there is no cash payment option here.[10] However, the analysis does not stop there. Since Kang's publication in 1998, customers seem to be more comfortable with the amount of data collection that happens when shopping online. If not more settled, customers are at least more aware of the manipulation of their shopping habits that manifests into banner ads for the next week. However, there is a new wave of data collection happening. The trend is reverting back to the brick and mortar stores as the most seamless and convenient shopping experience. These new types of brick and mortar stores have similar data collection processes to cyberspace that are hidden within the architecture;[11] they are the "eStores." As emphasized earlier, newer technology correlates to greater data collection and greater privacy concerns, and the consumer's lack of knowledge about this collection shifts the American shopper into the third wave of shopping space.

1. Brick and Mortar Stores Prior to the Wave of Online Shopping

The biggest concern customers had in brick and mortar stores prior to the emergence of online shopping was when making their purchase at the point-of-sale. When a customer swipes a credit card at a reader to make a purchase, the machine reads the magnetic strip holding the customer's personal information. The ease of fraudsters acquiring credit card data was most apparent to consumers in the wake of two major retailers being hacked.[12] In November 2013, Target revealed that up to 110 million customers were affected by malware found from their point-of-sale devices giving unauthorized access to payment card data.[13] Weeks later, Neiman Marcus acknowledged that 1.1 million of its customers were also affected by malicious software.[14] While data breaches are unfortunately common, the amount of damage done in these instances was unique because of the large number of people that were affected by these breaches.

Courts have not always been sympathetic towards customers who have been involved in credit card hacks. Retailers have not been held liable if they complied with bank regulations on magnetic stripe data storage.[15] However, amendments have been made to the law to help protect consumers against potential data breaches. In 2003, the Fair Credit Reporting Act was amended to truncate credit and debit card numbers to

10. *Id.*
11. *See* Lawrence Lessig, *Code* 43 (Version 2.0 2006).
12. Byron Acohido, *Timeline: Target, Neiman Marcus disclosures*, USA TODAY (Feb. 6, 2014), http://www.usatoday.com/story/cybertruth/2014/01/23/timeline-target-neiman-marcus- disclosures/4799153/.
13. *Id.*
14. *Id.*
15. *Cumis Ins. Society, Inc. v. BJ's Wholesale Club, Inc.*, 455 Mass. 458 (Sup. Jud. Ct. Mass. 2009) ("the system is designed with the expectation that breaches will occur.").

help maintain anonymity with the number on a receipt, but this does not apply to electronic receipts.[16] In reaction to the stream of recent data

Breaches, banks will be issuing Europay, MasterCard, Visa ("EMV") credit cards,[17] which have PIN and chip technology that cards in Europe already have. By October 2015, retailers are expected to change their credit card readers to be able to accept these safer cards, which will rely on cryptographic keys to encrypt information and PINs to verify customers rather than the magnetic stripe.[18]

2. eCommerce and Mobile Apps

When customers go on any webpage, they are traced by tiny files and programs called "cookies."[19] There are two types of cookies: first-party and third-party. First-party cookies are collected by the direct website that the user is browsing on.[20] Third-party cookies track a customer's movement throughout all sites affiliated with the track company, and the company can collect information about the person to create a profile on the customer.[21] Third-party cookies are usually the greater privacy concern.[22] Once the cookies pick up the data, the data is used in algorithms that can help further connect the personal information that is collected with probable behavior data such as income, geographic location, and education.[23] This information can not only help them further personalize ads, correspondence, and offers, but it also can put together independently anonymous information to identify an individual.[24] Companies like Amazon use this data as a recommendation mechanism by monitoring everything that their customers do transactionally and even noting information on the purchases that are not

16. 15 U.S.C. § 1681(g)(1).
17. Susan Johnston, *Coming Next Fall: More Chip and PIN Cards in the U.S.*, US NEWS (Oct. 28, 2014), http://money.usnews.com/money/personal-finance/articles/2014/10/28/coming-next-fall-more-chip-and-pin-cards-in-the-us. ("The technology is also referred to as EMV, which stands for Europay, MasterCard and Visa, the three card brands that created the chip in Europe and Canada.").
18. *Id.*
19. Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL STREET JOURNAL (July 30, 2010), http://www.wsj.com/articles/SB10001424052748703940904575395073512989404.
20. Marc Groman, *First- Or Third-Party Cookie? Wrong Question*, ADEXCHANGER (Dec. 10, 2013), http://adexchanger.com/data-driven-thinking/first-or-third-party-cookie-wrong-question/.
21. Angwin, *supra* note 19.
22. Groman, *supra* note 20 ("Although the first party brought in the third party to provide a service that it believed to be beneficial…the third-party data collection in this scenario is assumed to present at potentially greater privacy risk to consumers.").
23. Angwin, *supra* note 19.
24. *Id.*

actually made.[25] Even though the consumer is providing a great amount of information, they are getting more accurate recommendations from Amazon.[26]

3. eStores

a. RFID

Beginning around 2012, retail stores began incorporating radio frequency identification ("RFID") tags into their products. RFID is used to replace bar codes to help in inventory management.[27] RFID tags are small electronic devices used to receive and transmit information from radio frequencies.[28] Using this technology makes the distribution of products and materials more beneficial by keeping track of inventory and limiting costs, which serves as a mutual benefit to consumers as well as businesses.[29] Beyond attaching to individual garments, RFID tags can be attached to materials used for shipping that can help let a manufacturer know where the products are until they reach the retailer.[30] A benefit to RFID tags is that they are reusable and can be removed from the garment at checkout, which is cost effective for retailers. By providing accurate information on the availability of inventory and how to avoid stock-outs, RFID technology elevates the modern day shopper's experience that expects to find what they want when they want it.[31] The technology takes some of the responsibility away from the employees so they can better assist customers.[32] Additionally, it assists retailers and manufacturers to better serve their retail spaces by looking at shopping patterns to make their supply chain more efficient.[33] It seems to be a win for both the consumer and the manufacturer.

---

25. Lou Carlozo, *How Online Retailers Collect & Use Consumer Data*, DEALNEWS (Dec. 23, 2013), http://dealnews.com/features/How-Online-Retailers-Collect-Use-Consumer- Data/938928.html.
26. *Id.* ("The megaretailer wants to drive the most meaningful offers to its users, so the more information it compiles, the more accurate Amazon's recommendations based on psychographics, demographics, or spending habits are. That's why we call it a win for the consumer.").
27. Charles J. Condon, *RFID and Privacy: A Look Where the "Chips" are Falling*, 11 Appalachian J.L. 101, 106 (2011).
28. *Id.* at 102.
29. *Id.* at 103.
30. *Id.* at 107.
31. Mark Hill, *How RFID Technology is Revolutionizing the Consumer Shopping Experience*, RETAIL TOUCHPOINTS (July 9, 2012), http://www.retailtouchpoints.com/executive-viewpoints/1711-how-rfid-technology-is-revolutionizing-the-consumer-shopping-experience-.
32. *Id.* ("It also enables better availability of a store's merchandize, which frees up associates to focus on the customer vs. the stockroom, creating a better shopping experience that ultimately fosters customer loyalty.").
33. *Id.*

Mass-market merchants such as Wal-Mart and J.C. Penney have adopted RFID technology into their inventory. However, RFID has also become very advantageous for fast fashion retailers.[34] For example, more than half of Zara stores currently have RFID technology, and all of their stores will have the technology by the end of 2016.[35] The efficiency and increased speed in production is key for a fast fashion company that relies on immediate production as a result of the latest trends right off the runway. Prior to the use of RFID, Zara's storewide inventories were every six months, but now they are performed every six weeks allowing Zara to get "a more accurate picture of what fashions are selling well and any styles that are languishing."[36] As items are sold, the technology immediately sends a restock order to the stockroom for that exact item without the employees having to do the work based on written sales reports.[37] Additionally, this technology allows salespeople to help find a product that might not be in that particular store, but can be located at another store or online.

b. Customer Tracking

Technology used inside stores is not only tracking the goods, it is tracking every movement people inside and outside of the store are making. These technologies generally use the Wi-Fi on a mobile device to connect to a customer, but sometimes the customer does not even have to connect to the store's server to be tracked.[38] One of the most commonly used trackers is Euclid Analytics ("Euclid"). Euclid has been described as the "Google Analytics for the real world" and detects foot traffic within retail locations.[39] Euclid connects to shoppers' smartphones through Wi-Fi or Bluetooth technology and collects the mobile device's media access control ("MAC") addresses.[40] MAC addresses are unique to each phone, and each

34. *See* Felipe Caro and Victor Martínez-de-Albéniz, *Who's Fast Fashion and Who's Not*, The UCLA Anderson Global Supply Chains Blog (Feb. 28, 2014), http://blogs.anderson.ucla.edu/global-supply-chain/2014/04/defining-and-measuring-fast- fashion.html.
35. Christopher Bjork, *Zara Builds Its Business Around RFID*, WALL STREET JOURNAL (Sept. 16, 2014), http://www.wsj.com/articles/at-zara-fast-fashion-meets-smarter-inventory-1410884519.
36. *Id.*
37. *Id.*
38. Eilene Zimmerman, *Bringing Digital Analytics to Main Street Retailers*, NEW YORK TIMES (Aug. 27, 2014), http://boss.blogs.nytimes.com/2014/08/27/bringing-digital-analytics-to-main- street-retailers/. (describing RetailNext technology).
39. Sarah Perez, *Euclid Elements Emerges From Stealth, Debts "Google Analytics For The Real World"*, TECH CRUNCH (Nov. 3, 2011), http://techcrunch.com/2011/11/03/euclid-elements- emerges-from-stealth-debuts-google-analytics-for-the-real-world/.
40. Sarah Perez, *Euclid, The "Google Analytics For The Real World," Partners With Aruba, Aerohive, Xirrus & Others To Make Tracking Sensor-Free*, TECH CRUNCH (Jan. 4, 2013), http://techcrunch.com/2013/01/04/euclid-the-google-analytics-for-the-

address is stored to the Euclid server.[41] 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.[42] In fact, Euclid provides retailers with a recommended sign to use in their retail space.[43] The information collected about a consumer, known as Mobile Location Analytics, tells the retailer how long a customer is in each part of the store and where they choose to browse.[44] Not only does that allow a retailer to strategize what products are more popular, it also allows the retailer to predict when the store will be busiest and how to use its sales staff more efficiently.[45] Additionally, Euclid can track the number of people that walk by a store window and how long they stand in front of the window before making the decision to go inside or continue walking.[46] This information is beneficial to a retailer to be able to adjust its window display to be more enticing to more customers.[47]

In 2013, Nordstrom, a major United States department store, received backlash for its use of Euclid resulting in the company's decision to stop using the technology in their stores.[48] Shoppers referred to the system as "creepy" and felt that they were being stalked in the store.[49] Interestingly, customers seem to have accepted the cookie collection and online profiles created when they use the Internet to make purchases.[50] This further shows the shift in the retail space and the unaddressed privacy concerns that Kang had not anticipated when he wrote his piece. At the time, brick and mortar and ecommerce seemed to be two separate shopping experiences, but the reality of the modern world is that the once separate forces have merged together.

---

real-world-partners-with- aruba-aerohive-xirrus-others-to-make-customer-tracking-sensor-free/.

41. *Id.*
42. *In-store Notice Guide lines*, EUCLID (Sept. 2014), http://euclidanalytics.com/resources/euclid_instorenotice_guideline_201409.pdf. (providing details on placement requirements for notices).
43. *Id.* ("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.").
44. Peter Cohan, *How Nordstrom Uses WiFi to Spy on Shoppers*, FORBES (May 9, 2013), http://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi- to-spy-on-shoppers/.
45. *Id.*
46. *Id.*
47. *Id.*
48. Stephanie Clifford and Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, NEW YORK TIMES (July 14, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper- stores-are-tracking-your-cell.html.
49. *Id.*
50. *Id.* ("some bristle at the physical version, at a time when government surveillance- of telephone calls, Internet activity and Postal Service deliveries- is front and center because of the leaks by Edward J. Snowden.").

Besides Euclid, another similar technology, RetailNext, also uses Mobile Location Analytics.[51] This system is even more precise and its technology can differentiate between men and women customers, as well as distinguish customers from employees.[52] RetailNext also has heat maps that detect the activity throughout the store.[53] The company website claims that their kinetic heat maps "[a]llow retailers to understand shopper movement in their stores, be it high- traffic areas, bottlenecks, or neglected areas that need attention."[54] Companies such as Bloomingdales, American Apparel, and Mont Blanc use RetailNext.[55] The newest development in the world of retail tracking is unpredictable, but it is clear that this growing trend will not stop. Beyond Mobile Location Analytics, retailers are using facial recognition technology to track customers within their stores.[56] FaceFirst poses itself as a source of security protection against shoplifters and organized retail criminals.[57] However, it is also promoted as a way to keep track of a store's most important customers and highest spenders.[58] Upon a customer's entrance into a store, a camera will take a picture of the customer's face, which will be added to the store's client database.[59] With the image in the database, the monitors will recognize the face every subsequent time the customer enters the store.[60] Upon recognition, the authorized person at the store will be alerted via email or text that the person has entered the premises.[61] Additionally, retailers can preset pictures of those that will be tracked in the system.[62] This can be particularly convenient for suspicious activity or to give a high spending customer some extra assistance.[63]

51. Press Release, 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/.
52. *Id.*
53. *Id.*
54. *Id.*
55. Jonathan Shieber, *RetailNext Raises Another $30 Million To Track In-Store Data*, TECHCRUNCH (July 8, 2014), http://techcrunch.com/2014/07/08/retailnext-raises-another-30-million-to- track-in-store-data/.
56. Services, Face First, http.//www.facefirst.com/services.
57. Retail, Face First, http://www.facefirst.com/services/retail.http://www.facefirst.com/services/retail.
58. *Id.*
59. David Lumb, *Is Facial Recognition The Next Privacy Battleground?*, Fast Company (Jan. 26, 2015), http://www.fastcompany.com/3040375/is-facial-recognition-the-next-privacy-battleground.
60. *Id.*
61. Natasha Singer, *When No One Is Just a Face in the* Crowd, NEW YORK TIMES (Feb. 1, 2014), http://www.nytimes.com/2014/02/02/technology/when-no-one-is-just-a-face-in-the-crowd.html.
62. *Id.*
63. *Id.*

c. Connected Store

While these individual technologies track products inside the store and how customers interact with them, all of this has combined to develop the new shopping experience for customers in retail stores—the smart store. In late 2014, designer Rebecca Minkoff, best known for her women's accessories, joined together with eBay to develop a project referred to as a "Connected Store."[64] So far, the San Francisco and New York locations have adopted this model. Upon entering the store, a customer is connected to the store through their smartphone.[65] A large touch screen greets customers at the entrance to allow them to browse through the store's inventory and select pieces to have sent to a dressing room.[66] Once their selected pieces are ready, the customer can opt to be alerted that their dressing room is ready via a cell phone alert.[67] While in the dressing room the customer will experience the RFID shields that detect that clothing is inside the room. Rebecca Minkoff stores in Los Angeles and Tokyo also have these dressing rooms.[68] The mirrors function as touch screens allowing the customer to customize the lighting in the room as well as select other clothing such as swapping their selection for a different size or color.[69] The customer can also use the touch screen to order something online if it is sold out in that store.[70]

Once the customer has completed their experience in the dressing room, the customer will be able to make the transaction on the sales associates' iPads. Customers can also use loyalty cards with their purchases. This transaction is designed to provide a very seamless point- of-sale experience; in fact, there are no traditional registers to make purchases in the store.

Meanwhile, the retailer is able to collect the information on what pieces were not purchased and later send follow-up messages to see if they would consider those pieces.[71] While the spread of these types of stores is still limited, this is the direction that retail shopping is moving towards. Shoppers are interested in making their shopping experience as seamless as possible, but naturally, with new and unfamiliar technology comes the privacy concerns of what information is being collected about the customers and how it will be used. It is important to look at privacy laws

64. Neal Ungerleidger, *Why Rebecca Minkoff And eBay Are Betting On Smart Dressing Rooms*, FAST COMPANY (Nov. 12, 2014), http://www.fastcompany.com/3035229/the-smart-dressing- room-experiment-how-irl-shopping-is-getting-less-private-but-more-persona. ("Minkoff and eBay are simply implementing a real-life version of the pervasive tracking and cookies that have become part and parcel of the e-commerce experience.").
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*

that currently apply to similar technologies as well as how to apply these regulations to the technologies used in the new way of stores.

II. THERE IS VERY LITTLE REGULATION CONCERNING THE COLLECTION OF DATA IN RETAIL STORES.

The amount of data that is collected by eStores sparks privacy concerns for consumers. Traditionally, privacy law has been thought of as four major torts: (i) unreasonable intrusion upon the seclusion of another; (ii) appropriation of the other's name or likeness; (iii) unreasonable publicity given to the other's private life; or (iv) publicity that unreasonably places the other in a false light before the public.[72] However, privacy rights are protected by state law, and not all states recognize all four torts. Out of the four torts, intrusion upon the seclusion of others embodies the concerns with the information collected by retail technologies. Intrusion upon seclusion is an intrusion into a person's private matters that are not of public concern, and this intrusion must be considered highly offensive by the reasonable person to be actionable.[73]

A. The Federal Trade Commission Provides Guidelines to Protect Personal Identifiable Information.

A major privacy concern with the gathering of customer information by retailers is that they are collecting highly sensitive person information known as personal identifiable information ("PII"). The United States Department of Labor defines PII as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."[74] This information can be isolated to identify an individual, such as a name, address, social security number, or phone number, or it can be a combination of elements that help to isolate a person among a group, such as gender, race, and geographic location.[75] Unauthorized access to this information is known as a breach of security and risks the harm of releasing PII.[76] Laws relating to PII are implemented in each state. While many are the same, some are stricter than others. California was the first to enact a data breach notification law in 2002, which required retailers to notify customers if

72. Restatement (Second) of Torts § 652A.
73. Restatement (Second) of Torts § 652B.
74. *Guidance on the Protection of Personal Identifiable Information*, UNITED STATES DEPARTMENT OF LABOR, http://www.dol.gov/dol/ppii.htm.
75. 18 U.S.C. § 1028(d)(7).
76. Cong. Research Serv., Data Security Breach Notification 1 (Apr. 10, 2012), http://fas.org/sgp/crs/misc/R42475.pdfhttp://fas.org/sgp/crs/misc/R42475.pdf ("unauthorized acquisition of personal information that compromises security, confidentiality, or integrity of personal information maintained by a covered entity").

there was a data breach that jeopardized their PII.[77] A delay or lack of disclosure would lead to criminal investigation. Almost all states now have some sort of notification law in place.

The Federal Trade Commission ("FTC") is permitted to regulate unfair methods of competition and unfair and deceptive acts in commerce.[78] The FTC has explained its approach to data security is based on a reasonableness standard.[79] The FTC set out four major guidelines for companies to follow in their collection of data: (i) knowing what information they have and

who has access to it; (ii) limiting the collection and retention of information to what is necessary; (iii) using secure methods to protect the information; and (iv) disposing information when it is no longer necessary.[80] Very few cases have been litigated with the FTC over data security and unfair practices. Currently, Wyndham Hotels & Resorts, LLC is litigating in the Third Circuit over the FTC's ability to bring an unfairness claim for data security.[81] The outcome of that decision could impact how data security is regulated in the United States as well as potentially leading to more FTC enforcement than before. To handle possible information leaks, the FTC has guides for businesses to help protect customer information and avoid security breaches and identity theft.[82] Additionally, under the Fair Credit Reporting Act, businesses that accept credit or debit cards are required to truncate or eliminate all but the last five digits of the card number on the customer's receipt at the point-of-sale.[83]

77. Cal. Civ. Code § 1798.29 ("Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose encrypted personal information was…acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay").
78. 15 U.S.C. § 45(a).
79. Federal Trade Commission, *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
80. *Id.*
81. *See generally F.T.C. v. Wyndham Worldwide Corp.*, 799 F. 3d 236 (3d Cir. 2015); *see also LabMD, Inc. v. Federal Trade Commission*, 776 F.3d 1275 (11th Cir. 2015) (finding that the District Court lacked jurisdiction to decide whether the FTC had exceeded its power to determine if a medical lab's data security practices were unfair).
82. *See generally* Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, November 2011, https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information- guide-business.
83. 15 U.S.C. § 1681c(g)(1).

B. eStores Must be Diligent and Transparent with the Data Tools they use in their Retail Stores and Properly Train their Employees to use These Tools.

1. RFID Tags

There is an inherent fear attached to any type of technology that has tracking capability. RFID tags on clothing and shipping containers track where items are going, until they are removed at the point of transaction. However, they are "passive with respect to the consumer."[84] The tags do not collect personal information about an individual; rather, the data collected is generic information about the products' level of demand, independent of information about the purchaser. Additionally, customers are less likely to be concerned with the tracking of the RFID technology because they are not likely to be aware of the tags.[85] Unlike other tracking devices, like cookies, that remind customers that they have looked at an item and considered it for purchase, RFID tags will not later remind customers that they had moved the product to the fitting room because the product will not be linked to the customer.

The biggest concern is to make sure that the RFID labels are removed at the point-of-sale.

It is arguably easy to overlook the tags because they are not readily apparent, and salespeople may not be aware of their existence. Having a customer walk out being tracked by the tags could be of concern as it would allow tracking of the customer's home address, which is a release of PII.[86] Beyond the retailer being able to track the customer outside of the store, anyone else with a RFID scanner could locate a tag, which is even more alarming.[87] Currently, there are no state laws that prohibit the use of RFID tags on products. However, some states have laws that prohibit third parties from reading PII extracted from RFID. Alabama,[88] California,[89] Illinois,[90]

84. *Supra* note 27, at 108. (quoting Paul J. Bruening, staff counsel for the Center for Democracy and Technology).
85. *Id.*
86. *Id.* at 117. ("While it may be a good idea for a retailer to use RFID chips to manage its inventory, we would not want a retailer to put those tags on goods for sale without consumers' knowledge, without knowing how to deactivate them and without knowing what information will be collected and how it will be used").
87. *Id.* (quoting Senator Bill Nelson of Florida) ("[m]ore disturbingly, anyone with powerful RFID scanners, including the government, potentially could use scanners to locate people in crowds, assuming the targeted person was carrying a product with an active RFID tag").
88. *See generally* AL Code § 13A-8-113 (2013).
89. *See generally* Cal. Civ. Code § 1798.79(a). ("A person or entity that intentionally remotely reads or attempts to remotely read a person's identification document using radio frequency identification (RFID), for the purpose of reading that person's identification punished by imprisonment in a county jail for up to one year, a fine…or both").
90. *See generally* 720 ILCS 5/16-30.

Nevada,[91] and Washington[92] all have state laws that make reading PII through a scanner of RFID a criminal violation. Transparency is key in letting customers know the limits of the tracking and what the tags will collect on these garments. Looking at RFID tags as they are used solely for purposes of assessing inventory, there does not seem to be major privacy concerns with which consumers would be uncomfortable if they were aware. However, whether other uses of RFID in the retail space pose bigger privacy risks will be discussed later. Europe has already developed extensive regulation since 2009 regarding RFID technology and the requirement for retailers to make customers aware of the use of RFID technology and what data is collected through the tags.[93] While the use of these tags will continue, disclosing what the tags are for, as is done throughout Europe, would put consumers at ease.

2. Consumer Tracking Devices

a. Mobile Location Analytics

In October 2013, the Future of Privacy Forum, United States Senator Charles Schumer, and companies involved with mobile location analytics announced that they had agreed to a Code of Conduct (the "Code") to tackle this new type of technology.[94] Euclid was one of the companies involved in the agreement. The Code ensured that there would be transparency with the information collected.[95] The Code limits the collection, retention, and distribution of the analytics. Additionally, companies using mobile location analytics must provide opt-in consent for PII that is collected and opt-out consent for non-personal information that is collected.[96] Companies will be

91. *See generally* Nev. Rev. Stat. § 205.46515.
92. *See generally* Rev. Code Wash. § 9A.58.020.
93. Press Release, European Commission, *Digital privacy: EU-wide logo and "data protection impact assessments" aim to boost the use of RFID systems* (July 30, 2014), http://europa.eu/rapid/press-release_IP-14-889_en.htm.
94. Joseph Jerome, *The Future of Privacy Forum and Sen. Schumer Announce Important Agreement to Ensure Consumers Have Opportunity to "Opt-Out" Before Stores Can Track Their Movement Via Their Mobile Devices,* THE PRIVACY FORUM (Oct. 22, 2013), http://www.futureofprivacy.org/2013/10/22/schumer-and-tech-companies-announce-important- agreement-to-ensure-consumers-have-opportunity-to-opt-out-before-stores-can-track-their- movement-via-their-cell-phones/; *see also* Siraj Datoo, *How tracking customers in-store will soon be the norm*, THE GUARDIAN (Jan. 10, 2014), http://www.theguardian.com/technology/datablog/2014/jan/10/how-tracking-customers-in-store- will-soon-be-the-norm (FTC praising the Code for helping to develop a self-regulatory code of conduct).
95. Future of Privacy Forum*, Mobile Location Analytics: Code of Conduct* (2013), http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf.
96. Laura Heller, *New registry lets shoppers opt-out of location analytics*, FIERCE MOBILE RETAIL (Feb. 18, 2014), http://www.fierceretail.com/mobileretail/story/new-registry-lets-shoppers-opt- out-

required to identify that they are using these types of technology, and it must be clearly explained in their company privacy policy.

Retailers have not received public support for implementing mobile location analytics. Nordstrom's decision to discontinue using Euclid's services was likely because of the negative press that the company received from its use, as seen in Forbes' article "How Nordstrom Uses WiFi to Spy On Shoppers."[97] In May 2014, Philz Coffee made the decision to stop using Euclid at its coffee shop.[98] Customers of the popular coffee shop did not seem pleased that their movements were being traced. Euclid Chief Executive Officer Will Smith maintains that Euclid never collects PII, stating that, "We're shoppers too, so we wanted to create a powerful product that helps retailers optimize the shopping experience, while at the same time could be proud of as consumers. We've built our technology from the ground up with privacy in the fore- front, and none of the information we collect can ever be traced back to an individual."[99]

However, the growing privacy concern with customer tracking services, like Euclid, is not direct PII, but various pieces of information that can become PII when put together if a customer does not opt-out, and as long as Euclid turns on every time they are near a store that uses the technology. Each person is given an anonymous customer identification number, which does not include personal information, but this identification number is always associated with that individual smartphone. Over time, the patterns of the person's visits can be put together to reveal information that identifies the person. For example, a person's sudden recent visits to stores that sell maternity clothes or baby items may indicate that the person is pregnant.[100] While Euclid maintains that its business does not have privacy concerns because no PII is being collected, the anonymity of the smartphone linked to the individual identification number is questionable. Even if information is collected and used for a particular purpose, the problem of unpredictable uses sparks concern because unless all the uses are limited, privacy must be sacrificed.[101] Additionally, the aggregation of

location-analytics/2014-02-18 ("This platform will give consumers the ability to seamlessly inform companies they do not want the identity of their devices used for analytics purposes").

97. Cohan, *supra,* note 44.
98. Kyle Russell, *Philz Coffee Drops Euclid Analytics Over Privacy Concerns*, TECH CRUNCH (May 29, 2014) http://techcrunch.com/2014/05/29/philz-coffee-drops-euclid-analytics-over-privacy- concerns/.
99. *Id.*
100. *See also*, Kashmir Hill, *How Target Figured Out a Teen Girl was Pregnant Before her Father Did*, Forbes (Feb. 16, 2012), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target- figured-out-a-teen-girl-was-pregnant-before-her-father-did/ (describing Target's historical data collection and analysis through its customer cards that knew a teenage girl was pregnant before her father did).
101. Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. Colo. L. Rev. 1117 (2013).

information with time could be concerning, particularly if a substantial portion of retail locations choose to implement Mobile Location Analytics.

California's Online Privacy Protection Act is one of the furthest reaching state laws regarding privacy policies for online services that collect personal information from California residents.[102] The privacy policy must explain the type of information that will be collected and explain the company's tracking practices. Historically, this has been associated with online shopping, but with the increased use of tablets and other computer systems within the brick and mortar store, companies will have to be aware of how this may change how they do business. So far, there has been no application of this with regard to retail stores, but it is a consideration that companies may have to be creative about. One way to approach this issue is to encourage customers to use the in-store Wi-Fi, which will then prompt the customer to accept the terms and

conditions of the data that will be collected when the customer's phone is using Wi-Fi , as well as store tablets and devices. Posting privacy policies throughout the store is also a way to maintain transparency. However, no matter what method is chosen, companies are recommended to obtain specific outside expertise on California regulation and how to avoid any potential violation.

b. Heat Detection

The use of heat detection in platforms like RetailNext raises additional concerns. While retail locations are not restricted under the Fourth Amendment, this type of information collection is parallel to the information collected in the precedential decision, *Kyllo v United States.*[103] In *Kyllo*, the United States Department of the Interior used thermal imagers to detect excessive warmth radiating from the petitioner's home due to high intensity lamps used for growing marijuana.[104] The Supreme Court found the use of heat detection technology to be an unlawful search.[105] The Court's dissent did mention that these rules could be applied to other private spaces beyond the home, such as a telephone booth or office building.[106] While this unreasonable search is limited to actions by the government and its agents, *Kyllo* can be used to consider the heat technology used by RetailNext. The dissent mentions private places beyond the home are to be "considered." The human body is a private place that requires protection from unnecessary intrusion. Accordingly, the heat detection of a human body in a store is as intrusive as the thermal imaging

102. The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).
103. *See Kyllo v. United States*, 533 U.S. 27 (2001).
104. *Id.* at 29.
105. *Id*. at 40.
106. *Id.* at 49 ("[A] rule that is designed to protect individuals from the overly intrusive use of sense-enhancing equipment should not be limited to a home.").

used at the outside of a home. While body heat is not a form of PII, its intrusion is still substantial and should be considered by future lawmakers that face these developing technologies.

c. Facial Recognition Technology

Facial recognition technology is used in people's everyday lives outside of the retail store. The major privacy concern is that facial recognition acquires biometric data, which is unique to an individual.[107] Whether or not third parties should have access to this type of biological data is a question that still has not been answered by the courts or lawmakers.[108] Further, if the stores can access this information there is concern that other unauthorized parties could obtain this information. Jennifer Lynch, legal counsel for the Electronic Frontier Foundation, remarks that a data breach that would allow access to this information would be more problematic than the Target data breach.[109] Lynch says it could impact "the fundamental values of being able to participate in society anonymously" because the information collected for a short-term coupon has a long-term life in the system keeping track of the customer's every move.[110] Lynch also identifies the issue of customers' ignorance about permitting stores to use their information, which further supports the need for customer education and complete transparency from retailers.[111]

3. Connected Store

a. Discount Cards Law

In 2000, Connecticut enacted the Consumer Discount Cards Law to prohibit retailers from selling or sharing consumer information that they gain from consumers, unless the retailer gave the customer reasonable notice and opportunity to opt-out.[112] The law applies to all types of retailers, including fashion retailers. California has a more stringent version of the law that is only applicable to supermarkets. The California law does not even require consumers to opt-out; rather the retailer cannot collect information about the customer, regardless of whether or not the customer

107. Lumb, *supra* note 59.
108. Singer, *supra* note 61 ("[L]ike DNA sequencing, it measures and records biological patterns unique to individuals. Like concerns over the proliferation of genetic data, the debate over facial recognition ultimately revolves around whether a person has a right to control who has access to his or her biometric data and how it can be used.").
109. Lumb, *supra* note 59.
110. *Id.* ("It's data that follows you: It's tracked in-store, tracked in the checkout counter, it might be linked to your credit card data…And all that might be sold to a third party.").
111. *Id.*
112. H.B. 5586, 2000 Leg. Sess. (Conn. 2000).

takes action to prevent it.[113] Connecticut classifies consumer information as that which identifies a consumer, or what is more commonly understood as PII.[114] The statute also defines discount cards as a device used by a customer to obtain a discount when making purchases.[115] It is not clear if loyalty cards are included under this statute, but it is certainly arguable. If companies choose to implement loyalty cards, retailers must be cautious not to relinquish this information to third parties and to clearly describe how the information will be stored. This type of regulation could limit how third parties analyze the benefit of the store through better understanding shopping patterns and gaining further information about customers who frequent its store.

b. Information Collected in the Transaction

Privacy concerns over credit card breaches have been apparent in retail stores even before smart stores were introduced. The Target and Neiman Marcus attacks were some of the biggest data breaches to date and changed customer's trust of these popular retailers. Trust, as will be discussed in Part IV, seems to be the key for a store to be successful in incorporating new technology that may raise privacy concerns with its customers. As a result of these data breaches, credit cards will switch to the chip-and-PIN cards by October 2015, which are already used in Europe.[116] Chip-and-PIN cards are significantly more secure than cards with magnetic strips due to the fact that it is more difficult to copy data from a chip.[117] Additionally, the PIN verification provides an additional layer of security for the user.[118] The chip-and-PIN cards have been effective in preventing card fraud in other countries.[119]

Beyond data breaches, retailers need to be aware of state specific laws that impact the data that is collected at the point-of-sale. The amount of data collected in stores has increased as stores are now inputting customer information for advertising and promotional purposes and maintaining records of customer transactions. This information often links back to the customer's phone number and email, sending customers coupons and discounts or general mass messages. California is notorious for its

113. Cal. Civ. Code § 1749.64
114. C.G.S.A. § 42-371.
115. *Id*.
116. Tom Risen, *Credit Cards Will Get Security Upgrade in* 2015, US News (Feb. 11, 2014), http://www.usnews.com/news/articles/2014/02/11/credit-cards-will-get-security-upgrade-in- 2015.
117. Douglas King, *Chip-and-PIN: Success and Challenges in Reducing Fraud* - Retail Payments Risk Forum Working Paper, FEDERAL RESERVE BANK OF ATLANTA (Jan. 2012), https://www.google.com/#q=Douglas+King%2C+Chip-and-PIN:+Success+and+Challenges+in+Reducing+Fraud%2C+Retail+Payments+Risk+Forum%2C+Jan.+2012.
118. *Id*.
119. *Id*.

protection of customer's data at the point-of-sale due to the Song-Beverly Credit Card ("Song-Beverly"), which prohibits the collection of PII by a retailer when accepting the credit card as payment.[120] Courts have applied a very broad definition of PII in cases relating to Song-Beverly. In 2011, a Williams-Sonoma customer sued the retailer for requesting her ZIP code, information thought to be necessary to complete the transaction.[121] A California court held that a ZIP code meets the qualifications of PII, and the store's request for the customer's ZIP code was a violation of Song-Beverly.[122] Retailers need to properly train their sales staff to abide by these particular state laws and be aware of how they impact the data that can be collected in the store. In fact, Rebecca Minkoff has been particularly cautious of monitoring the collection of phone numbers or other personal information in the store and at what times the information is requested to avoid violations of Song-Beverly.[123]

c. RFID in Dressing Rooms and More

Much like the clothing in many retail stores using RFID technology, the clothing in smart stores, such as Rebecca Minkoff's, contains RFID on the tags. As discussed above, the privacy concerns are minimal so long as the tags are properly removed once the customer's transaction is complete. However, smart stores are relying on RFID technology for reasons beyond the restocking of inventory. For example, dressing rooms in the Rebecca Minkoff smart stores have a RFID reader hidden into the light fixtures in the dressing room.[124] The RFID tags in the garments will be read by the RFID reader in the light fixture. A screen laid over the mirror then displays that specific garment.[125] The customers are given the option to input their mobile number into the screen in the dressing room to keep track of what items were tried on.[126]

This is all possible because of the RFID readers. The trouble comes with the collection of the phone number, a form of PII. While customers are opting-in by voluntarily providing their information,[127] most customers are unaware of how this information is kept and how the data collected about

120. Cal. Code § 1747.08.
121. *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 528 (2011); *see also Korn v. Polo Ralph Lauren Corp.*, 644 F. Supp. 2d 1212, 1218 (E.D. Cal. 2008) (finding that Song-Beverly only applies to transactions and not to refunds).
122. *Pineda*, 51 Cal. 4th at 534.
123. Telephone Interview with Craig Fleischman, Corporate Development, Rebecca Minkoff (May 1, 2015).
124. Claire Swedberg, *Rebecca Minkoff Store Uses RFID to Provide an Immersive Experience*, RFID JOURNAL (Nov. 21, 2014), http://www.rfidjournal.com/articles/view?12445/.
125. *Id*.
126. *Id*.
127. Constant Contact, Confirmed Opt-In Guide (Mar. 2008), https://www.constantcontact.com/aka/docs/pdf/confirmed_optin_user_guide.pdf.

their shopping preferences can impact their future experiences with the company. The hidden RFID reader is aesthetically clean, but it also makes it even less obvious to the customer about the extent of the technology used in the store. Opt-in policies are a great way for companies to collect information about their customers without the privacy concerns of the opt-out process; however, individuals should be aware of exactly what information is being collected and how it will be used. If companies are requesting mobile numbers, the customer should agree to a terms of use before the cell phone number is collected.

Additionally, there are reports that Rebecca Minkoff employees will soon have handheld RFID readers to carry around the store to collect information about inventory that is available on the store floor.[128] However, the RFID readers will pick up on any RFID labels, including those placed on the clothes that are held by the customers in the store. Having more people with the ability to monitor and precisely track the movements of the people within the store seems intrusive and could impact surveillance laws. Further concern is sparked by the ability of anyone with a RFID reader to be able to pick up these signals including the government.

Americans are protected under the Fourth Amendment from unwarranted searches and seizures, which also applies to electronic surveillance.[129] The Electronic Communications Protection Act provides remedies for those who have been subject to unlawful electronic surveillance.[130] Retail stores should be cautious of the number of employees who have access to this type of technology and should be diligent in training the employees to only collect data of necessity and not beyond. Losing the loyalty and trust of a customer over the collection of excess data could have a dramatic effect on the profitability of a retail store.

III. eSTORES SHOULD DEVELOP SELF-REGULATORY SCHEMES TO ADDRESS PRIVACY CONCERNS WITH THE CUSTOMER DATA THAT IS COLLECTED.

Lawmakers are discussing the changes happening in the retail space. Senator Charles Schumer has called retailer tracking of buyers "intrusive and unsettling."[131] While the FTC regulates deceptive or unfair conduct that companies engage in, the FTC has yet to bring any enforcement actions against a fashion company for tracking.[132] Without any regulatory or legal precedent it is difficult to determine if companies are crossing the line with the collection of this data. This poses two major questions: (i) Does the

128. Swedberg, *supra* note 109.
129. *See, e.g.,* Katz v. U.S., 389 U.S. 347 (1967).
130. 18 USC § 2701.
131. Ungerleidger, *Supra* note 64 ("If you're shopping, you expect to be the one doing the reviewing, but stores are flipping that on its head.").
132. Matthews, *supra* note 3.

definition of PII need to be expanded? and (ii) Are customers ready to accept the technological capabilities of these shopping enhancing services?

The California courts have used a wider interpretation of PII, but it seems that PII may need to be expanded to less specific information that can still be used to identify people. Data collection, particularly by mobile location analytics systems, are allowed in these practices because they are not collecting what has been defined as traditional PII. Non-PII can be pieced together with other information to personalize the information and connect it to a particular individual.[133] A new approach to PII has been explained as information that has a good possibility of future identification.[134]

Perhaps this also can change depending on the retailer that is collecting information.

Luxury brands have fewer customers coming through the store as opposed to Wal-Mart. Additionally, luxury brands offer limited goods so the collection of information on individuals may not be as meaningful. The customers entering the doors of a Hermès store can likely afford a $10,000 Birkin bag, otherwise they would not be coming into the store. Whereas in a megastore like Wal-Mart or Costco, the placement of items within the store or selection of what brands to feature within the store requires data and information that is incredibly valuable to the store. The definition of PII is best viewed on a case-by-case basis. As courts and the FTC continue to regulate data collection, there will likely be a shift in what is perceived as PII.

Based on the reaction of Nordstrom and Philz Coffee customers to the mobile location analytics tracking services, it is clear that not all customers like the idea of being monitoring by retailers. Consumers have already taken steps to remain anonymous with their Internet browsing by deleting cookies or using false information to create personal accounts for email or social media.[135] Public awareness of the National Security Agency's data collection or data breaches like those at Target and Neiman Marcus have made consumers more alert about the information that is being collected about them,[136] and there has been resistance by customers to allow their information to be collected. A particular concern that customers have is how the information will be used. In fact, Rebecca Minkoff has been

133. Paul M. Schwartz and Daniel J. Solove, *PII 2.0: Privacy and a New Approach to Personal Information*, THE BUREAU OF NATIONAL AFFAIRS INC. (2012), http://docs.law.gwu.edu/facweb/dsolove/files/BNA-PII-FINAL.pdf ("This phenomenon of data availability heighten the ability to turn non-PII into PII.").

134. *Id*.

135. Lee Rainie, Sarah Kiesler, Ruogu Kang, and Mary Madden, *Anonymity, Privacy, and Security Online*, PEW RESEARCH CENTER (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

136. Glenn Greenwald, *Major opinion shifts, in the US and Congress, on NSA surveillance and privacy*, THE GUARDIAN (July 29, 2014), http://www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew.

particular about which technologies it has incorporated into its current Connected Stores and which technologies it anticipates introducing once customers are "ready."[137] The reality is that most stores can easily be equipped with advanced technologies, but retailers must be cautious not to scare away customers with the technology. This type of gradual introduction of technology shows that retailers are cognizant of their customer's concerns. Beyond the data collection and analysis by retailers, data brokers have built an entire industry based on selling information collected about consumers. Data brokers are engaged in collecting information as a third-party about individuals and selling it to agencies or companies.[138] Data brokers use information from government and public records, self-reported information from consumers from contests or surveys, social media, or even from other participating companies.[139] There are no laws that prevent retailers from using the information from data brokers or preventing the selling or exchange of this information,[140] and even if customers are made aware of data collection that is happening within their stores they may not be aware of the information that is being used by the store that the store did not directly collect from the customer.[141] The FTC's response to data brokers has been to publicize FTC complaints and orders in order to educate companies and consumers of the need to disclose how this information is used.[142] Education accompanied by time to become acclimated to this type of collection is necessary to ensure transparency for consumers.

Even though some customers have heightened awareness around the information that is collected about them, customers have also become accustomed to having a highly personalized shopping experience and expect these types of services from their retailers.[143] Some customers are

137. Telephone Interview with Craig Fleischman, Corporate Development, Rebecca Minkoff (May 1, 2015).
138. Privacy Rights Clearinghouse, *Fact Sheet 41: Data Brokers and Your Privacy* (Apr. 1, 2015), https://www.privacyrights.org/content/data-brokers-and-your-privacy.
139. *Id.*
140. *See* Federal Trade Commission, FTC's Data Brokers A Call for Transparency and Accountability (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
141. *Getting to know you*, THE ECONOMIST (Sept. 13, 2014), http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly- followed-advertisers-and-third-party.
142. Federal Trade Commission, What Information Do Data Brokers Have on Consumers, And How Do They Use It (Dec. 18, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal- trade-commission-entitled-what-information-do-data-brokers-have- consumers/131218databrokerstestimony.pdf.
143. Grace Nasri, *Why consumers are increasingly willing to trade data for personalization*, DIGITAL TRENDS (Dec. 10, 2012) http://www.digitaltrends.com/social-media/why-consumers-are-increasingly-

willing to give up their personal information for the perks that companies will give them, even if they are unaware of how the information is being collected.[144] Consumers are willing to trade their personal information if it means they will be rewarded with exclusive perks and coupons.[145] A Seattle based company developed a mobile app that gave customers cash and gift cards in exchange for information about where the customer was in a store.[146] The app has gained a significant following despite selling customer's gender, age, and income to store owners, online retailers, and app developers. There is a hard balance between what customers want in their shopping experience and what they are willing to give up to get these benefits. However, customers should not feel hopeless with the growing world of technology and data collection. In fact, customers do have tools to prevent or allow information to be collected about them.

California's privacy-related laws are the broadest and most robust, but they have an overall theme of providing as much information as possible to the people whose privacy is being impacted. The key to harmonizing the tension between customers and retailers is transparency,[147] which is what California laws seem to be emphasizing. The more information that is made available to consumers, the more comfortable they will feel because it is no longer a hidden secret. There are a great number of people who are unaware of this information, and a leak of their information can feel like a violation of their rights. However, providing disclaimers that can be easily understood in a direct and non-intimidating manner will help to develop a trusting relationship between retailers and customers. Relationships between retailers and customers are just like any other type of relationship: to be sustained they must be built on trust.

The reality is that data collection is not going to slow down, but customers need to have the ability to control their data. Customers can turn off Wi-Fi and Bluetooth services to prevent mobile location analytics from working,[148] but this is impractical because consumers are likely to forget. However, companies participating in the Code allow customers to opt-out of their services by registering online.[149] This seems like the more practical solution for customers to protect themselves with one opt-out rather than voluntarily adjusting their phone setting every time they are in a retail

willing-to-trade-data-for-personalization/ ("A personalized web experience is something that most have become accustomed to; whether it is from a curated news feed, targeted flash sales, or even designing your own product directly on a site.").

144. Clifford, s*upra* note 48 (describing Philadelphia blogger who wasn't aware of tracking methods. She remarks that retailers are "trying to sell, so that makes sense.").
145. *Id*.
146. *Id*.
147. Jake Williams, *FTC calls for transparency in data collection*, FEDSCOOP (May 27, 2014), http://fedscoop.com/ftc-calls-transparent-data-collection/.
148. Fact Sheet 41, *supra* note 123.
149. Future of Privacy Forum, Mobile Location Analytics Opt Out (2014) http://smart-places.org/.

space. The importance of clear opt-out procedures is apparent in the consent order between Nomi Technologies, a mobile location analytics tracker, and the FTC.[150] Nomi recently settled with the FTC over investigation that Nomi was not properly allowing opt-out mechanisms for in-store collection of data, even though Nomi had a clear opt-out mechanism on their website.[151] This stresses the importance of complying with opt-out procedures. Additionally, there is some push to allow the collection of data but to use it in an aggregate way. Rather than pinpointing individual patterns, looking at a group of people to indicate a trend can be more beneficial to a company's strategy and simultaneously protect the identities of the customers they are monitoring.[152]

The FTC has already begun regulation with Nomi Technologies[153] and further regulation will continue as the public and the regulators become more aware of the privacy concerns. President Obama has recently reintroduced the Consumer Privacy Bill of Rights, which would govern the collection and distribution of data.[154] The bill would help consumers keep track of the information that is collected about them and require companies to be transparent about the information that they collect.[155] However, because data collection is so new to society, perhaps allowing the self-regulation that has begun with the aid of the FTC and the Code is an appropriate measure at this time. Self-regulation is in the interest of retail stores for policy reasons and business reasons. The FTC's *Fair Information Practice Principles* are guidelines for online entities to provide notice, consent, access, security, and enforcement in a self-regulatory manner to protect consumers.[156] While these guidelines are supported by other federal and state law, the success of a self-regulatory regime is based on providing clear rules that consumers understand are followed by the private sector and have recourse if they are not followed. As the alternative to strict federal or state laws, it would be beneficial for retail stores to develop a regulatory mechanism to provide consistency throughout the industry and show

150. *See* Consent Order, Federal Trade Commission v. Nomi Technologies, Inc., No. 1323251 (Apr. 23, 2015), https://www.ftc.gov/system/files/documents/cases/150423nomiorder.pdf.
151. *Id*.
152. Ellen Rooney Martin, *The Ethics of Big Data*, FORBES (Mar. 27, 2014) http://www.forbes.com/sites/emc/2014/03/27/the-ethics-of-big-data/.
153. *See* Complaint, Federal Trade Commission v. Nomi Technologies, Inc., No. 1323251, https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf.
154 Andrew Lustigman and Adam Solomon, *An overview and the impact of the Consumer Privacy Bill of Rights*, INSIDE COUNSEL (Mar. 12, 2015), http://www.insidecounsel.com/2015/03/12/an-overview-and-the-impact-of-the-consumer- privacy.
155. *Id*.
156. Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

initiative in complying with these practices. If the retail industry does not self-regulate it will only be a matter of time until lawmakers make the rules for them. Based on the customer reaction to Nordstrom and Philz Coffee, it is in the retail stores' best interests to be honest with their customers to cultivate consumer loyalty to increase business; after all, increasing business is the reason retail stores use these technologies in the first place. Customers have been receptive to the collection of information over the Internet because they are aware of it; they either choose to take measures to protect themselves or have accepted that this is what must be sacrificed to have a more efficient shopping experience. Time will only tell, but it seems that customers will soon be accepting of the eStore as they become more educated about the data collection practices.

CONCLUSION

The evolution of the eStore is a shopping experience that customers should be eager to embrace. If retailers want to run the most efficient business based on the data they collect about their customers, they must always put the customer first by prioritizing the customer's right to know what data is being collected. Shoppers will continue to make purchases in brick and mortar stores even as they become eStores, but transparency will help cultivate and maintain the type of relationship that will be most mutually beneficial for both parties.