SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 1, PAGE 1

HOW MUCH DOES J. CREW REALLY KNOW ABOUT YOU?: THE HARSH REALITY OF A MEGA-RETAILER'S PRIVACY POLICY

Laura Fleming

ABSTRACT

This paper seeks to illustrate what a typical privacy policy of a mass retailer looks like, as very few people actually bother to read a website's privacy policy. Also, accompanying each section of the privacy policy, this note will discuss the consequences each section has on consumers, as well as solutions for better protecting privacy. The second half of this paper will focus on the different methods available to consumers for enforcing their privacy rights. Furthermore, we will we look at a bill, which, while it ultimately did not pass, offered good solutions for best protecting consumer privacy. While this bill was not successful, it will undoubtedly help provide the framework for future privacy laws. Finally, this note will discuss measures that consumers, who wish to protect their personal information from retailers, can take, until Congress enacts suitable privacy laws.

INTRODUCTION

Nowadays, one cannot visit an online shopping website which does not display a privacy policy. A privacy policy is a statement that declares a website's policy on the collection and release of information about a visitor.[1] Privacy policies usually state what specific information the company collects and whether this information is kept confidential, shared, or sold to third parties.[2] However, very few people actually take the time to read through the privacy policy and consider its implications.[3] While most retailers provide links to its privacy policy, and most companies send an email to subscribers when the company updates the policy, the link is usually in small font at the bottom of the page; thus, many website visitors never even notice that the policy is available for viewing.

Despite the growing number of online retailers, there are very few laws regulating companies' use of customers' personal information.[4] Most states, with the exception of California, do not require retailers to provide privacy policies.[5] However, while state law may not require a retailer to post a privacy policy, federal law might.[6] For example, by the Children's Online Privacy Protection Act (COPPA), websites that collect personal information from

---

[1] BUS. DICTIONARY, http://www.businessdictionary.com/definition/privacy-policy.html (last visited Feb. 16, 2014).

[2] *Id.*

[3] Shankar Vedantam, *To Read All Those Web Privacy Policies, Just Take A Month Off Work*, NAT'L PUB. RADIO (Apr. 19, 2012, 3:30 AM), http://www.npr.org/blogs/alltechconsidered/2012/04/19/150905465/to-read-all-those-web-privacy-policies-just-take-a-month-off-work.

[4] Robert V. Connelly Jr., *Are Online Privacy Policies Required By Law?*, THE RVC BLOG (Oct. 25, 2010), http://www.rendervisionsconsulting.com/blog/are-online-privacy-policies-required-by-law/#sthash.i0K1u5fv.dpuf.

[5] *Id.*

[6] *Id.*

children under the age of thirteen must provide a privacy policy.[7] Nevertheless, this widespread lack of regulation leads to a lack of privacy, which this society values highly.

Accordingly, this paper will step through the privacy policy of one of America's largest online retailers, J.Crew, and explain the implications of each section on the customer. J.Crew's online store brought in over $134 million in revenue in 2012 and offers online shopping in 107 countries.[8] In addition, J.Crew's website rated the strongest for customer service speed and quality.[9] This adds to J.Crew's already great online reputation and draws even more customers to its online shop.

Furthermore, this paper will examine the options available to consumers who are concerned for their privacy, due to the ever-expanding collection of personal information by retailers. Then, this paper will discuss a recent bill, which attempted to protect consumers by implementing consumer-friendly policies regarding privacy policies. Finally, this paper will identify precautions and steps customers can take to protect their personal information from being used to their disadvantage by retailers seeking to cash in.

---

[7] *Children's Privacy*, BUREAU OF CONSUMER PROT. BUS. CTR., http://www.business.ftc.gov/privacy-and-security/children%27s-privacy (last visited Feb. 16, 2014).

[8] Lydia Dishnman, *Inside J. Crew's Move Back to Black*, FORBES (AUG. 30, 2012, 4:22 PM), http://www.forbes.com/sites/lydiadishman/ 2012/08/30/inside-j-crews-move-back-to-black/; Stephen Cotterill, *'Hello, World,' J.Crew says, via the web*, INTERNET RETAILER (June 27, 2014, 2:34 PM), http://www.internetretailer.com/2012/06/27/hello-world-jcrew-says-web.

[9] Lorna Pappas, *J.Crew, L.L. Bean And Net-A-Porter Among Best Online Customer Serv. Providers*, RETAIL TOUCHPOINTS (Sept. 11, 2013), http://www.retailtouchpoints.com/in-store-insights/2871-jcrew-ll-bean-and-net-a-porter-among-best-online-customer-service-providers.

I. ANALYSIS OF J.CREW'S PRIVACY POLICY

A. Collection Of Information

1. Information You Provide

The first section of J.Crew's privacy policy states that J.Crew collects information that customers provide.

> For example, [J.Crew] collect[s] information when you use [its] websites, shop in [J.Crew's] stores, call [J.Crew] on the phone, create an online account, sign up to receive…emails, request a catalog, participate in a sweepstakes, contest, promotion or survey, communicate with [J.Crew] via third party social media sites, request customer support, apply for a job or otherwise communicate with [J.Crew]. The types of information [J.Crew] may collect include your name, email address, zip code, billing address, shipping address, phone number, payment card information, product preferences, demographic information and any other information you choose to provide. In some cases, [J.Crew] may also collect information you provide about others, such as when you purchase a gift card for someone…, create and share a "wish list" or decide to purchase and ship products to someone. [J.Crew] will use this information to fulfill your requests and will not send marketing communications to your contacts unless they separately opt in to receive communications from [J.Crew].[10]

While consumers are most likely aware of the ramifications of providing information, such as a phone number or email address, there is one piece of information that may seem harmless to provide, but which, in fact, is not harmless. This unlikely source of personal information is the customer's ZIP code.[11] When a customer provides a retailer with this five-digit number, the customer opens the door to an abundance of junk mail and telemarketing calls.[12] As a result, Paul Stephens, the director of policy and advocacy for Privacy Rights Clearinghouse, a nonprofit watchdog group based in San Diego, California, recommends saying "no" when asked

---

[10] *Privacy Policy*, J.CREW, https://www.jcrew.com/help/privacy_policy.jsp (last visited Feb. 16, 2014) [hereinafter J.CREW).

[11] A. Pawlowski, *Should You Tell Stores Your ZIP code? Privacy Advocates Say No*, CNBC (Mar. 19, 2013, 2:14 PM), http://www.cnbc.com/id/100569424.

[12] *Id.*

for your ZIP code by a retailer.[13] This is because when a retailer pairs your ZIP code with your name, it can determine your mailing address, phone number, and specific demographic information.[14] Therefore, while a customer may believe they are only providing their ZIP code to the retailer, they are actually providing the company with much more personal information.

Accordingly, retailers are able to transform a ZIP code into valuable personal information through direct marketing services companies, such as Harte-Hanks, which offers the GeoCapture service to retailers.[15] Therefore, once the retailer obtains the customer's name from running their credit card and obtains the customer's ZIP code, this service "matches the collected information to a comprehensive consumer database to return an address."[16] Now armed with customer addresses, retailers can send mail marketing directly to customers.[17]

In response to these services, Massachusetts and California declared this practice violates their privacy laws.[18] These states ruled that a ZIP code amounts to "personal identification information."[19] However, while a customer can refuse to give their ZIP code while shopping in-

[13] *Id.*

[14] *Id.*

[15] Adam Tanner, *Never Give Stores Your ZIP Code. Here's Why*, FORBES (June, 19, 2013, 8:19 AM), http://www.forbes.com/sites/ adamtanner/2013/06/19/theres-a-billion-reasons-not-to-give-stores-your-zip-code-ever/.

[16] *Id.*

[17] *Id.*

[18] Pawlowski, *supra* note 11.

[19] *Id.*

store, online it is much more difficult.[20] This is because you need to provide a ZIP code for your shipping and billing addresses.[21]

However, there is an option for online shoppers who are required to provide their ZIP code in order to receive their package. A customer can opt out of most solicitations by registering with the Direct Marketing Association's Mail Preference Service.[22] Nevertheless, belonging to any database does open you up to the small risk that your information could be part of a wholesale data theft and ultimately used to steal your identity.[23]

Another valuable, yet more obvious, source of information for retailers is a customer's email address. For that reason, most retailers display a box on its homepage where patrons can sign up to receive emails from the company.[24] However, once a user enters their email address, most companies redirect the customer to a form where the company requests even more information.[25] Further requested information typically includes address, gender, preferred store, date of birth, and ZIP code.[26] As for J.Crew, this retailer offers an email sign-up box at the bottom right hand side of its webpage, and once one enters their email address they are redirected to a screen that asks for their first and last name, ZIP code, and country.[27] Therefore,

---

[20] *Id.*

[21] *Id.*

[22] Marlys Harris, *Asking for Your ZIP Code: A New No-No for Retailers?*, CBS MONEY WATCH (Feb. 17, 2011, 5:24 PM), http://www.cbsnews.com/8301-505145_162-38140938/.

[23] *Id.*

[24] David Moth, *Email sign up forms: a look at how 16 fashion retailers collect customer data*, ECONSULTANCY (July, 24, 2013), http://econsultancy.com/us/blog/63124-email-sign-up-forms-a-look-at-how-16-fashion-retailers-collect-customer-data.

[25] *Id.*

[26] *Id.*

[27] *See* J.CREW, *supra* note 10.

by obtaining a customer's name and ZIP code, J.Crew can send this information to direct marketing service companies to obtain even more personal information about the customer.

2. Information the Retailer Collects Automatically

The second section of J.Crew's privacy policy relates to information the company collects automatically whenever a customer visits its website or transacts business with the company.[28] The policy states that J.Crew collects information about:

> your use of [its] websites, such as the type of browser you use, access times, pages viewed, your IP address and the referring link through which you accessed [J.Crew's] websites…[Also,] [w]hen you purchase or return a product, [J.Crew] collect[s] information about the transaction, such as product details and the date and location of the purchase/return…[Additionally, J.Crew] may use cookies…and other tracking technologies to collect information about you when you interact with [J.Crew's] websites…, including information about your browsing and purchasing behavior. [J.Crew] may combine this information with other information [it] collect[s] about you and use it for various purposes, such as improving [its] websites and your online experience, understanding which areas and features of [its] sites are popular, counting visits, understanding campaign effectiveness, tailoring [its] communications with you, determining whether an email has been opened and links within the email have been clicked and for other internal business purposes.[29]

For this section of J.Crew's privacy policy, this paper will focus on retailers' use of customer return information, browser cookies, cell-phones, and IP addresses for collecting customer information.

While most people are aware that a retailer requests a customer's email address at the register or online with intent to keep the customer informed of promotions and track their purchase history from the company, most customers are not aware that information tracking

---

[28] *Id.*

[29] *Id.*

customer returns is just as important for retailers.[30] Nonetheless, since consumers return about $264 billion worth of merchandise each year, which is equivalent to almost 9% of total sales, retailers want to be able to identify chronic returners or gangs of thieves trying to make off with high-end products that are returned later for store credit.[31]

Thus, when one goes to make a return at a store, most retailers ask to see the customer's driver's license.[32] Typically, the information taken from a customer's license includes the identification number, the customer's name, address, date of birth, and expiration date.[33] This is because retailers collect customer return information and outsource that information to third parties, such as The Retail Equation, which create "return profiles" of customers.[34] These "return profiles" catalog and analyze the customer's returns at the store and online.[35] While customers consider this practice an invasion of privacy, the retail industry defends its practices, "claiming that this method is used to fight theft, not monitor its shoppers."[36] Bob Schoshinski, Assistant Director of the Federal Trade Commission's Division of Privacy and Identity Protection, stated that "[m]ost people think when they hand over a driver's license that it's just to confirm identity and not to be kept to be used for future transactions;" however, "[i]t shouldn't be that a third

[30] Jennifer C. Kerr, *Retailers keeping tabs on consumers' return habits*, YAHOO! FINANCE (Aug. 12, 2013, 3:27 PM), http://finance.yahoo.com/news/retailers-keeping-tabs-consumers-return-115934658.html.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] Kerr, *supra* note 30.

[36] *Id.*

party is keeping a profile on someone without them being informed what's going to happen when they hand over their driver's license or some other information to a retailer."[37]

Consequently, once the retailer receives a customer's "return profile," if there is a pattern of questionable returns, which suggests possible fraud, the retailer could then deny returns by that shopper at the store for a certain period of time, determined by the retailer.[38] The Retail Equation claims, however, that once the company analyzes consumer information, it only reports back to the specific retailer that requested the information, not all retailers that use the service.[39]

Nevertheless, consumers are not happy with this information sharing technique. However, lawsuits in this area have been ineffective.[40] In 2011, a man filed a lawsuit against Best Buy after the store swiped his driver's license for a return.[41] The man requested that the manager delete the information, to which he refused.[42] Thus, the plaintiff alleged that Best Buy violated privacy law when it swiped the license. However, a federal appeals court held that the Driver's Privacy Protection Act did not apply in these circumstances.[43]

As for tracking technologies, one common type of tracking used by retailers is "browser cookies." Browser cookies are text files that gather information about a computer user's Internet habits.[44] Browser cookies "contain unique identifiers and associate 'browsing history

---

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] Kerr, *supra* note 30.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] Bose v. Interclick, Inc., No. 10 Civ. 9183(DAB), 2011 WL 4343517, at *1 (S.D.N.Y. Aug. 17, 2011).

information' with particular computers."[45] Advertising networks use this browsing history information to create "behavioral profiles."[46] Thus, when a computer user visits a web page, on which the advertising network provides advertisements, the advertising network uses a behavioral profile to select particular advertisements to display on that computer.[47]

Furthermore, if you've ever noticed an item you looked at online reappear in an ad on another website, this is because online retailers assign customers a virtual identification number and track customers as they go from site to site.[48] As a result, retailers "purchase targeted ads for products they already know you're strongly interested in."[49]

An explanation of the way this advertising occurs is as follows: First, commercial websites rent out online advertising "space" to other websites.[50] Then, in the simplest arrangement, the host website rents space on its web pages to another website, which allows the website to place a banner advertisement on the web page.[51] Next, when a user on the host website clicks on the banner advertisement, the user is automatically connected to the advertiser's website.[52] Thus, companies, such as DoubleClick, act as intermediaries between the host websites and websites seeking to advertise.[53] These companies promise retailers that they

---

[45] *Id.*

[46] *Id.*

[47] *Id.* at *1.

[48] Christopher Matthews, *Future of Retail: How Companies Can Employ Big Data to Create a Better Shopping Experience*, TIME (Aug. 31, 2012), *available at* http://business.time.com/2012/08/31/future-of-retail-how-companies-can-employ-big-data-to-create-a-better-shopping-experience/.

[49] *Id.*

[50] *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502 (S.D.N.Y. 2001).

[51] *Id.*

[52] *Id.*

[53] *Id.*

will "place their banner advertisements in front of viewers who match their demographic target."[54] This is possible because, when users visit any of these affiliated websites, a "cookie" is placed on their hard drives.[55] Afterward, the companies' cookies store this personal information on users' hard drives until it can electronically access the cookies and upload the data.[56] Once companies such as DoubleClick collect information from the cookies on users' hard drives, it compiles the information to build demographic profiles of users.[57] Then, DoubleClick and its licensees target banner advertisements using these demographic profiles.[58]

Consumers who are apprehensive about the practice of tracking "browser cookies" have two solutions. First, computer users can delete or block their "browser cookies," which prevents third parties from associating the user's browsing history information with their subsequent web activity.[59] Second, the computer user can visit the host website and request an "opt-out" cookie, which informs the website not to install third party advertiser cookies on the user's browser.[60]

Appropriately, there has been much litigation in this area under the Electronic Communications Privacy Act; however, this litigation has not been successful for consumers. As one court noted, "cookie[s]…are much akin to computer bar-codes or identification numbers

---

[54] *Id.*

[55] *DoubleClick,* 154 F.Supp. 2d at 502-03.

[56] *Id.* at 503.

[57] *Id.* at 505.

[58] *Id.* at 504-05.

[59] *Id.*

[60] *DoubleClick,* 154 F.Supp. 2d at 504; *Manage Cookies, What is an Opt Out Cookie?*, ALL ABOUT COOKIES, http://www.allaboutcookies.org/manage-cookies/opt-out-cookies.html (last visited Nov. 15, 2014).

placed on 'business reply cards' found in magazines."[61] While these bar-codes and identification numbers are "meaningless to consumers", they are "valuable to companies in compiling data on consumer responses."[62]

For example, in *In re DoubleClick*, a class action lawsuit was brought against DoubleClick, "the largest provider of Internet advertising products and services in the world," alleging violations of the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and state law claims of trespass and unjust enrichment.[63] There, the "[p]laintiffs allege[d] that DoubleClick's cookies collect[ed] 'information that Web users, including plaintiffs and the Class, consider to be personal and private.'"[64] This information included customer names, e-mail addresses, addresses, telephone numbers, searches performed on the Internet, websites visited on the Internet, and "information that users would not ordinarily expect advertisers to be able to collect."[65] However, the court found that DoubleClick's cookies only collected information regarding users activities on DoubleClick-affiliated Web sites.[66] Also, DoubleClick never accessed files, programs, or other information on users' hard drives.[67] Additionally, DoubleClick did not collect information from a user who took the steps to opt-out of DoubleClick's tracking.[68]

---

[61] *DoubleClick*, 154 F. Supp. 2d at 513.

[62] *Id.*

[63] *Id.* at 500, 513; 18 U.S.C. § 2701 (2002).

[64] *DoubleClick*, 154 F. Supp. 2d at 503.

[65] *Id.*

[66] *Id.* at 502-03.

[67] *Id.* at 504.

[68] *Id.* at 503.

Thus, in order for DoubleClick's actions to be considered unlawful access to stored communication by 18 U.S.C.A. §2701, the cookies long-term residence on users' hard drives must be considered "electronic storage."[69] Section 2510(17) defines "electronic storage" as: "(A) any *temporary, intermediate storage* of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication *by an electronic communication service* for the purpose of backup protection of such communication."[70] However, "the cookies' residence on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not 'electronic communication service' providers."[71] Therefore, customers' cookies and identification numbers are not protected; thus, DoubleClick cannot be held liable for obtaining them.[72] In addition, the court found that the plaintiffs offered no proof to support their assertion that Doubleclick's access was unauthorized.[73] Instead, the facts alleged supported the position that DoubleClick-affiliated websites did authorize DoubleClick's access, since "the very reason clients hire DoubleClick is to target advertisements based on users' demographic profiles."[74] Therefore, the court dismissed the case with prejudice.[75]

Subsequently, in *Bose v. Interclick*, Bose alleged that Interclick used "flash cookies" (or Local Shared Objects ("LSOs")) to back up browser cookies.[76] According to the Computer Fraud

[69] *DoubleClick*, 154 F. Supp. 2d at 511.

[70] *Id.*

[71] *Id.*

[72] *Id.* at 513.

[73] *Id.* at 510.

[74] *DoubleClick*, 154 F. Supp. 2d at 510.

[75] *Id.* at 526.

[76] Bose v. Interclick, Inc., No. 10 Civ. 9183(DAB), 2011 WL 4343517, at *1 (S.D.N.Y. Aug. 17, 2011).

and Abuse Act (CFAA), "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer ... shall be punished."[77] Under § 1030(a)(5)(C), the CFAA also subjects someone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage," to criminal liability.[78] However, the court held that the collection of demographic information does not "constitute[ ] damage to consumers or unjust enrichment to collectors."[79] In addition, the court likened advertising on the Internet to advertising on television or in newspapers.[80] Thus, even if Bose took steps to prevent the data collection, the plaintiff's injury is still insufficient to meet the statutory threshold.[81]

Another type of tracking technology that is on the rise is the collection of customer information through their cell phones. When customers shop in-store, stores are collecting information about customer shopping habits "using video surveillance and signals from [consumers] cell phones and apps to learn information as varied as their sex, how many minutes they spend in the…aisle and how long they look at merchandise before buying it."[82] This tracking is possible through companies such as RetailNext, which collects data from shoppers' smart phones in order to track shopping patterns.[83] Therefore, if a shopper has the Wi-Fi on their

---

[77] 18 U.S.C. § 1030(a)(2)(C) (2008).

[78] 18 U.S.C. § 1030(a)(5)(C) (2008); *Bose*, 2011 WL 4343517, at *3.

[79] *Bose*, 2011 WL 4343517, at *3 (citing *DoubleClick*, 154 F. Supp. 2d at 525).

[80] *Id.*

[81] *DoubleClick*, 154 F. Supp. 2d at 497; *Bose*, 2011 WL 4343517, at *5.

[82] Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July, 14, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&_r=0.

[83] *Id.*

phone turned on, a store that offers Wi-Fi is able to place the shopper's location in the store, even if the shopper does not connect to the network.[84] However, the use of tracking on smart phones makes many people uncomfortable.[85] Nevertheless, marketing through smart phones is believed to be the next big thing for retailers.[86] This is because "smartphones can bridge the gap between the online and offline worlds…[as] users always have their phones with them, even when they're not browsing the Internet."[87] Thus, "[r]etailers can learn about a customer through their online shopping behavior and then offer them short-term discounts through a cell-phone when the consumer is near that store[']s brick-and-mortar location."[88]

Nevertheless, it all comes down to retailers attempting to get consumers to buy more. While brick-and-mortar stores once cringed at the thought of customers using their phones to compare prices at competitor stores, now retailers are creating and publicizing their own mobile apps and offering in-store Wi-Fi.[89] Through these mobile apps, retailers can provide shoppers with coupons as they move throughout the store.[90] Also, Wi-Fi enables retailers to track the potential customer's online movements, which can further help retailers tailor advertisements and promotions to the specific consumer.[91]

---

[84] *Id.*

[85] Matthews, *supra* note 48; Chris Moran, *4 Ways Retail Stores Are Monitoring Your Every Move*, CONSUMERIST (Mar. 27, 2013), http://consumerist.com/2013/03/27/4-ways-retail-stores-are-monitoring-your-every-move/.

[86] Matthews, *supra* note 48; Moran, *supra* note 85.

[87] *Id.*

[88] Moran, *supra* note 85.

[89] Associated Press, *Technology digs deeper into personal shopping habits*, DENVER POST (Nov. 29, 2013), *available at* http://www.denverpost.com/nationworld/ci_24621678/technology-digs-deeper-into-personal-shopping-habits#ixzz2rQkFXHKh (last visited Nov. 15, 2014) [hereinafter *Technology digs deeper*].

[90] *Id.*

[91] *Id.*

While consumers are less worried about websites tracking their cookies, "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."[92] However, most Americans are willing to let companies access their personal data when provided with an incentive, such as additional savings or better service.[93] Yet, in response to customer complaints about this invasion of privacy, some retailers halted their cell phone tracking due to bad publicity.[94] On the other hand, some retailers claim that data collected at the point-of-sale "provides sufficient information without sparking the debate over individual consumers' privacy."[95]

Finally, another common tracking technology used by retailers is the determination of a consumer's approximate location. This is possible because a consumer's IP address can identify his approximate location.[96] Also, if a consumer is using a wireless connection, Wi-Fi triangulation can determine a consumer's location by surveying nearby wireless networks.[97] Not surprisingly, there is much concern over the tracking of location information, because it can pose a substantial privacy risk.[98] For example, by being able to reveal your whereabouts at any given

[92] Clifford, *supra* note 82.

[93] Ann Meyer, *Some Retailers Pull Back on Personalized Data Collection*, RETAIL LEADER, http://www.retailleader.net/top-story-tech___logistics-some_retailers_pull_back_on_personalized_data_collection-2294.html (last visited Nov. 15, 2014).

[94] *Id.*

[95] *Id.*

[96] *Online Privacy: Using the Internet Safely*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/online-privacy-using-internet-safely (last visited Nov. 15, 2014) [hereinafter *Online Privacy*].

[97] *Id.*

[98] *Id.*

time, it can be dangerous for individuals being stalked or domestic violence victims.[99] However, consumers can block their IP address through services such as Tor.[100] Also, consumers can use a Virtual Private Network (VPN), which replaces the IP address with one from the VPN provider.[101]

iii. Information Collected from Partners or Other Sources

This section authorizes J.Crew to obtain customer information from other sources and combine that information with information J.Crew collects about its customers.[102]

> For example, [J.Crew] collect[s] information from the U.S. Postal Service's national change of address database to verify and update mailing addresses. In addition, if you apply for a J.Crew credit card, [J.Crew] obtain[s] limited information about you from the partner that manages [its] co-brand credit card program.[103]

Therefore, J.Crew can discover what addresses to send catalogues or coupons to by matching customer names with the U.S. Post Offices' database. In addition, J.Crew can receive spending information and habits from the company that manages its store credit card. The purpose of this practice is to ensure customers are receiving promotions and communications, thus making them more likely to make a purchase.

---

[99] *Id.*

[100] *Id.*

[101] *Online Privacy*, *supra* note 96.

[102] J.CREW, *supra* note 10.

[103] *Id.*

B. Use of Information

Once J.Crew collects information about its customers from the numerous sources discussed above, J.Crew uses that information for a variety of purposes.[104] J.Crew states that it uses customer information in order to:

> Facilitate and improve your in-store and online shopping experience; Provide the products and services you request, process transactions and send you related information, including confirmations and receipts; Respond to your comments, questions and requests and provide customer service; Communicate with you about products, services, offers, promotions, rewards and events and provide news and information we think will be of interest to you…; Manage your online account(s) and send you technical notices, updates, security alerts and support and administrative messages; Personalize your online experience and provide advertisements, content or features that match your profile and interests; Monitor and analyze trends, usage and activities; Process and deliver contest, promotion and sweepstakes entries and rewards; Link or combine with information we get from others to help understand your needs and provide you with better service; and [c]arry out any other purpose for which the information was collected.[105]

This section of the policy also states that customers "consent to the processing and transfer of information in and to the U.S. and other countries" when one accesses J.Crew's website or provides the company with personal information.[106]

There are two main types of practices that retailers use to track customer behavior through the methods discussed above. The first is "behavioral targeting."[107] Behavioral targeting is "the practice of collecting and compiling a record of individuals' online activities, interests, preferences, and/or communications over time."[108] Using the methods already discussed, such as cookies, retailers are able to "monitor individuals, the searches they make, the pages they visit,

---

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Online Privacy*, *supra* note 96.

[108] *Id.*

the content they view, their interactions on social networking sites, and the products and services they purchase."[109] Then, retailers use this information to display advertisements to a customer, based on their behavioral record.[110] These advertisements are "based upon an individual's web-browsing behavior, such as the pages they have visited or the searches they have made."[111] Behavioral targeting is growing and replacing "contextual marketing," which is when retailers target users with advertisements that are based only upon the given webpage's content.[112]

The second type of tracking used by retailers is known as "dynamic pricing."[113] Dynamic pricing is when a retailer charges "different prices to different consumers for identical goods or services."[114] This is also possible through the use of cookies.[115] Retailers are able to read the cookies on a customer's browser to determine what products a consumer searched for and bought and how much the consumer paid.[116] Using this information, the retailer predicts how much a customer might be willing to spend on a product.[117] Also, some retailers consider other factors when determining pricing.[118] For example, retailers may charge inflated prices to customers who

---

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Online Privacy*, *supra* note 96.

[113] *Online Shopping Tips: E-Commerce and You*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/online-privacy-using-internet-safely (last visited Nov. 15, 2014) [hereinafter *Online Shopping Tips*].

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Online Shopping Tips*, *supra* note 113.

make repeated returns.[119] This price adjusting is legal as long as determination of the prices is not made based on race, religion, or gender.[120]

However, there are multiple strategies a consumer can use to defeat both "behavioral targeting" and "dynamic pricing." Consumers can combat behavioral targeting through the methods discussed above, such as deleting cookies and opting out. As for dynamic pricing, first, customers should not log into a site before obtaining a price quote.[121] Also, by clearing the cookies from your browser before you visit a site, retailers will not be able to match up your past browsing history.[122] In addition, by visiting sites from different browsers, consumers can see if the prices are the same across the board.[123] Finally, by using price comparison sites, which check prices from multiple vendors, consumers can see if they are being offered an inflated price on one website.[124] Undoubtedly, the main purpose of either practice is to sell more products.

C. The Sharing of Your Information

The third section of J.Crew's privacy policy outlines the situations in which the company may share information about its customers.[125] This section states that J.Crew can share customer information with:

---

[119] *Id.*

[120] Khadeeja Safdar, *Online Retailers Track Consumer Spending Habits To Get Wealthier Customers To Spend More*, THE HUFFINGTON POST (July, 25, 2012, 5:26 PM), http://www.huffingtonpost.com/2012/06/29/online-retailers-track-spending-habits_n_1637679.html.

[121] *Online Shopping Tips*, *supra* note 113.

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] J.CREW, *supra* note 10.

> vendors, consultants and *other service providers* who need access to such information to carry out work on [J.Crew's] behalf;…[J.Crew's] business partners and other third parties for purposes of sending their own direct mail, *unless you opt out of this type of sharing by logging into your online account and changing your preferences* or by contacting [J.Crew]; In response to a request for information if [J.Crew] believe[s] disclosure is in accordance with any applicable law, regulation or legal process, or as otherwise required by any applicable law, rule or regulation; If [J.Crew] believe[s] your actions are inconsistent with [its] user agreements or policies, or to protect the rights, property and safety of [J.Crew] or any third party; In connection with, or during negotiations of, any merger, sale of company assets, financing or transfer of all or a portion of [J.Crew's] business to another company; and [w]ith your consent or at your direction. [J.Crew] may also share aggregated or de-identified information, which cannot reasonably be used to identify you (emphasis added).[126]

This section of the privacy policy authorizes J.Crew to share customer information with third parties. This includes the third party that J.Crew contracts out to in order to place advertisements on other websites of products previously viewed on J.Crew's website.[127] For example, one of these companies, Acerno, has 140 million people in the United States on file in its database.[128] This company tracks what Internet users buy and view and then uses this information to place advertisements on more than 400 websites on behalf of retailers.[129] Like the companies described earlier, Acerno builds files linked to an identification number and places cookies on the browsers of Internet users who visit websites within its network.[130] However, Acerno requires online retailers that use its service to disclose its practices in its privacy

---

[126] *Id.*

[127] *Id.*

[128] Saul Hansell, *What Online Stores Sell: Data About You*, N.Y. TIMES (Oct. 24, 2008, 8:53 AM), http://bits.blogs.nytimes.com/2008/10/24/what-online-stores-sell-data-about-you/?_r=0 (last visited Nov. 15, 2014).

[129] *Id.*

[130] *Id.*

policy.[131] Also, Acerno requires its retailer customers to provide users the option to not have their shopping data tracked.[132]

This section also covers the sharing of consumer information with an analytics firm that "digest[s] and analyze[s] all the 'big data' that retailers and others collect."[133] While some retailers, such as Nordstrom, invest in internal data analysis, most use the software provided by large analytic firms.[134] Retailers input customer information into this software in order to adjust its marketing to meet consumer demand and better understand what products to place on clearance.[135] This is possible because the software considers factors such as inventory counts, customer views, and items viewed but not ordered, among others.[136]

In addition, companies in the same line of business are increasingly sharing information between one another.[137] This type of data sharing is valuable to companies because "by scaling the information base to include a much more comprehensive dataset of customers as well as non-customers' behavior…resources could be created and accessed which are impossible to generate internally."[138] Accordingly, these "comprehensive datasets" are seen as "proprietary and a source

---

[131] *Id.*

[132] *Id.*

[133] Mohana Ravindranath, *Brooks Brothers, national retailers analyze 'big data' from sales to adjust marketing*, WASH. POST (Sept. 22, 2013), *available at* http://articles.washingtonpost.com/2013-09-22/business/42299416_1_brooks-brothers-analytics-sales-data.

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] John Tengberg, *Inter-Organizational Information Sharing of Customer Data in Retail* (May 2013) (Composite Info. Sys. Lab., Working Paper No. 2013-09), *available at* http://web.mit.edu/smadnick/www/wp/2013-09.pdf.

[138] *Id.* at 14.

of competitive advantage."[139] However, this type of data sharing could have unfortunate effects on consumers. This is because the more databases a consumer's information is in, the greater the probability this information could be stolen.

D. Advertising, Security, and Children

The next three sections of J.Crew's privacy policy deal with advertising, analytics services, security, and children.[140] First, J.Crew expressly states that the company engages third parties to serve advertisements on its behalf.[141] J.Crew clearly provides that the third parties (i.e. companies such as Ascerno) may use cookies, IP addresses, pages viewed, and links clicked in order to collect information about J.Crew's customers.[142] Then, J.Crew expressly claims that this information will be used to deliver advertising targeted to a customer's interests on not only J.Crew's website, but other websites as well.[143] Also, just as Ascerno requires, J.Crew offers the option to consumers of opting out of Internet-based ads or opting out of having web-browsing information used for behavioral advertising purposes.[144] J.Crew then links Network Advertising's website so customers can easily opt-out of tracking.[145]

---

[139] *Id.*

[140] J.CREW, *supra* note 10.

[141] *Id.*

[142] *Id.*

[143] *Id.* (After being on J.Crew's website for purposes of this paper, advertisements showed up on multiple websites I visited thereafter, including my personal email account.)

[144] *Id.*

[145] J.CREW, *supra* note 10.

Second, J.Crew states that it will take "reasonable measures" to protect consumer information from theft, misuse, and unauthorized access.[146] However, the policy does not state what J.Crew considers a "reasonable measure."

Lastly, J.Crew states that it does not collect personal information from children under the age of thirteen.[147] This is consistent with federal law governing information collection of children.[148]

E. Consumer Choices

The final section of J.Crew's privacy policy deals with the choices available to consumers pertaining to online account information, promotional communications, cookies, and California privacy rights.[149] The part dealing with online account information states that,

> [y]ou may update, correct or delete your online account information at any time by logging into your account and navigating to the "My Account" page or by contacting [J.Crew]. You can also contact [J.Crew] if you wish to deactivate your online account, but note that [J.Crew] may retain certain information as required by law or for legitimate business purposes. [J.Crew] may also retain cached or archived copies of information about you for a certain period of time.[150]

Thus, this section about online account information offers consumers the option of deleting their online account with J.Crew. However, J.Crew states that it may still keep information about its customers, even after they delete their online account. Suspiciously, J.Crew does not state how long it will keep this information about its customers or for what purpose

---

[146] *Id.*

[147] *Id.*

[148] *Children's Privacy*, *supra* note 7.

[149] J.CREW, *supra* note 10.

[150] *Id.*

J.Crew will use this information, other than generic "business purposes." Also, this section does not affect the information that J.Crew gathered from the customer's in-store shopping; therefore, J.Crew may still have and may still use personal information, such as the customer's name and ZIP code.

Next, the section of J.Crew's privacy policy pertaining to promotional communications states that customers can

> opt out of receiving promotional communications from [J.Crew] at any time…To opt out of direct mail (such as catalogs and post cards): Log into your online account and adjust your settings under the "Catalog Preferences" page or contact [J.Crew]. To opt out of promotional emails and text messages: Follow the instructions provided in those communications or contact [J.Crew]. Please note that even if you opt out of receiving promotional communications, [J.Crew] may continue to send you non-promotional emails, such as those about your account or [J.Crew's] ongoing business relations.[151]

Thus, this section about promotional communications offers consumers the option of opting out of email and direct mail correspondence with J.Crew. However, like the previous section, J.Crew states that it may still keep information about its customers, even after they opt-out of receiving communications. Also, J.Crew still retains the right to send customers, who opt-out of promotions, emails about their account for ambiguous "ongoing business relations." The vague "catch-all" provisions in this section and the previous section demonstrate the need for more transparency in privacy policies and the necessity for laws that require this transparency.

Furthermore, the privacy policy also states that customers can set their browsers to

> remove or reject cookies, but note that doing so does not necessarily affect third party flash cookies used in connection with [J.Crew's] websites. For more information about disabling flash cookies, see www.adobe.com/products/flashplayer/security. Please note that if you choose to remove or reject cookies, this could affect the availability and functionality of [J.Crew's] websites…If you enable Do Not Track, J.Crew will not use information about your web viewing activities to tailor your online experience on other websites operated by J.Crew…[H]owever,…[J.Crew's] third party advertising providers may continue to use information about your web viewing activities to tailor advertising to

[151] *Id.*

> your interests across different websites even when you have Do Not Track enabled in your browser.[152]

This section informs customers of the options available to them for preventing tracking, such as the methods discussed previously. However, J.Crew casts the choice of "opting out" of cookies in a bad light. By claiming that J.Crew cannot "tailor your online experience" if you opt out of cookies, J.Crew makes it seem as if customers are missing out on a custom online "experience." This is because J.Crew, and all retailers, gain major benefits, such as the one's discussed above, from tracking consumers' cookies.

Finally, under the section dealing with California privacy rights, the policy states that:

> residents of California…[may] request certain details about how their information is shared with third parties for direct marketing purposes. Under the law, a business must either provide this information or permit California residents to opt in to, or opt out of, this type of sharing. J.Crew permits California residents to opt out of having their information shared with third parties for direct marketing purposes. To opt out, please log into your online account and change your settings under the "Catalog Preferences" page or contact [J.Crew].[153]

This section exists because, currently, California is at the forefront of privacy policy laws benefiting consumers, which is hopefully a path other states will soon follow.[154]

II. THE NEED FOR PRIVACY POLICIES

In a time when privacy concerns are front and center, with recent headlines including the theft of mass numbers of customer information from Target and data leaks by Edward Snowden, the lack of laws dealing with privacy policies is concerning. With the exception of a couple states, most states do not have regulations governing privacy policies, and neither does federal

---

[152] *Id.*

[153] *Id.*

[154] Michelle Quinn, *California Driving Internet Policy*, POLITICO (Oct. 8, 2013, 5:06 AM), http://www.politico.com/story/2013/10/california-internet-privacy-policy-97964.html.

law, except in limited circumstances. In the United States, online privacy is based on a concept called "notice and choice."[155] This means that websites may gather and use consumer information, as long as consumers are informed and have the option to opt out of it.[156] However, there is a major problem with this system.[157] The problem is the fact that this system assumes that website users read the privacy policy, which is often not the case.[158]

A. Potential Lawsuits

As we have seen with J.Crew's privacy policy, privacy policies enable companies to collect all sorts of personal information about not only customers, but potential customers as well. Thus, simply by providing a privacy policy, retailers are authorized to track a consumer's every move online and in store. In response to the wide range of methods companies are using to collect consumer information, consumers, concerned for their privacy rights, have brought many lawsuits. As the cases previously discussed have shown, typically, lawsuits are brought under one or more of four categories. These categories include the Computer Fraud and Abuse Act, a state's consumer protection act, trespass to chattels, and unjust enrichment.[159]

First, under the Computer Fraud and Abuse Act, a claimant must prove that"[w]hoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains

---

[155] Hansell, *supra* note 128.

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] *See* Del Vecchio v. Amazon.com, Inc., C11-366RSL, 2012 WL 1997697 (W.D. Wash. June 1, 2012).

anything of value ... shall be punished."[160] While this is predominately a criminal statute, it also provides for a civil cause of action.[161] However, to succeed on a civil cause of action, the conduct must involve at least one of the following factors: "loss to 1 or more persons during any 1-year period aggregating at least $5,000 in value;" "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;" "physical injury to any person;" "a threat to public health or safety;" "damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security;" or "damage affecting 10 or more protected computers during any 1-year period."[162] Nevertheless, it is usually difficult for a claimant to prove any one of these factors.[163] Arguably, the easiest factor to prove would be a loss of at least $5,000; however, the $5,000 cannot include "non-monetary detriments."[164] Accordingly, a court held that a claimant cannot argue that their private information has "economic value [equal to or] far in excess of $5,000," since their information was "economically exploitable" by the company.[165] Thus, the collection of private information alone is not enough to succeed under the Computer Fraud and Abuse Act.

Second, while states vary on what they require under their Consumer Protection Act, typically a claimant must prove "an unfair or deceptive act or practice,…injury to the plaintiff in

---

[160] *Del Vecchio*, 2012 WL 1997697 at *3; 18 U.S.C. § 1030(a)(4), (e)(2) (2008) (defining the term "protected computer" to include any computer "used in or affecting interstate or foreign commerce or communication").

[161] *Del Vecchio*, 2012 WL 1997697 at *3; 18 U.S.C. § 1030(g) (2008).

[162] *Id.*

[163] *Id.* at *4.

[164] *Id.*

[165] *Id.*

his or her business or property, and a causal link between the unfair or deceptive act and the injury suffered."[166] However, a claimant can allege an injury only if they can demonstrate that the company accessed the claimant's computer without authorization.[167] This is difficult to prove because typically the company's privacy policy notifies visitors of its actions (i.e. placing browser and Flash cookies on users' computers and using those cookies to collect information about the users' navigation and shopping habits).[168] Also, if the claimant made a purchase on the company's site, courts appear to conclude that action is sufficient acknowledgment "that cookies were being received and [there was] an implied acceptance of that fact."[169]

Third, under the tort theory of trespass to chattels, a party must prove intentional interference with the claimant's personal property, which deprives the owner of possession.[170] However, the one who intentionally interferes with the other's chattel is subject to liability only if "his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected…"[171]

[166] *Del Vecchio*, 2012 WL 1997697 at *6; *see* Gorbey ex rel. Maddox v. Am. Journal of Obstetrics & Gynecology, 849 F. Supp. 2d 162, 165 (D. Mass. 2012) (applying Massachusetts law); *see also* Goshen v. Mut. Life Ins. Co. of N.Y., 774 N.E. 2d 1190, 1193 (N.Y. 2002).

[167] *Del Vecchio*, 2012 WL 1997697 at *6.

[168] *Id.*

[169] *Id.*

[170] *Id.* at *8; *see* Sch. of Visual Arts v. Kuprewicz, 771 N.Y.S. 2d 804, 807 (N.Y. Sup. Ct. 2003).

[171] *Del Vecchio*, 2012 WL 1997697 at *8.

Therefore, plaintiffs may only prevail on this theory if the company sends thousands of requests to claimant's computer each day, or if the company's cookies bombard the claimant's computer with pop-up advertisements to the extent that viewing a webpage becomes impossible.[172]

Finally, under unjust enrichment, a claimant must prove that "(1) one party…conferred a benefit to the other; (2) the party receiving the benefit…[has] knowledge of that benefit; and (3) the party receiving the benefit…accept[ed] or retain[ed] the benefit under circumstances that make it inequitable for the receiving party to retain the benefit without paying its value."[173] Thus, "a person who is unjustly enriched *at the expense of another* is liable in restitution to the other."[174] However, courts have never considered the collection of demographic information, which is valuable for retailers, to constitute damage to the claimant or unjust enrichment to the collector.[175]

Nevertheless, while privacy policy lawsuits are mostly unsuccessful, most state and federal courts will hold a company to its privacy policy.[176] Therefore, if a company does something in contrast to its stated privacy policy, the company will likely be held accountable.[177] Also, many states have laws that hold companies liable for knowingly making a false or misleading statement in its privacy policy.[178] For example, in September of 2013, "users accused

---

[172] *Id.*

[173] *Id.* at *9; *see* Peterson v. Cellco P'ship, 80 Cal. Rptr. 3d 316, 323 (Cal. Ct. App. 2008); *see also* Mandarin Trading Ltd. v. Wildenstein, 944 N.E. 2d 1104, 1110 (N.Y. 2011).

[174] *Del Vecchio*, 2012 WL 1997697 at *9.

[175] *Id.*

[176] Robert V. Connelly Jr., *Are Online Privacy Policies Required By Law?*, THE RVC BLOG (Oct. 25, 2010), http://www.rendervisionsconsulting.com/blog/are-online-privacy-policies-required-by-law/#sthash.i0K1u5fv.dpuf.

[177] *Id.*

[178] *Id.*

Google of violating federal and state laws by intercepting people's emails in order to serve them ads that match keywords in messages."[179] Google defended its practices by claiming that users consented to email scanning when they accepted the company's terms of service.[180] However, Google's argument was unsuccessful on a summary judgment motion, because "Google didn't clearly explain to users that it might send ads based on email content."[181] This is because, even though Google "reserved the right to 'pre-screen' content," Google's privacy policy implied that content would be screened only to filter out objectionable material, not serve users targeted ads.[182] This ruling was said to reflect a "very consumer-friendly view of the privacy policy."[183]

Additionally, in December of 2013, users accused Apple of violating consumer protection laws by failing to follow its privacy policy.[184] However, the same judge that ruled on the Google lawsuit said, "consumers couldn't proceed without proof that they had read Apple's privacy policies."[185] This is troublesome because the law assumes that both parties to an agreement have read it.[186] Therefore, this ruling might indicate trouble for consumers who want to bring private lawsuits.[187]

---

[179] Wendy Davis, *Judge Rules Gmail Ads Might Violate Privacy*, MEDIAPOST (Sept. 26, 2013, 6:02 PM), http://www.mediapost.com/publications/article/210095/judge-rules-gmail-ads-might-violate-privacy.html.

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] *Id.*

[184] Wendy Davis, *Will Consumers' Loss Against Apple Affect Other Privacy Cases?*, MEDIAPOST (Dec. 5, 2013, 6:32 PM), http://www.mediapost.com/publications/article/214932/will-consumers-loss-against-apple-affect-other-p.html.

[185] *Id.*

[186] *Id.*

[187] *Id.*

B. Possible Reforms for Privacy Policy Laws

Accordingly, there clearly needs to be reform in the area of privacy policies, since consumer lawsuits are generally unsuccessful, and even lawsuits based on violations of privacy policies are not reliable. Consumers deserve to have a foolproof option of protecting themselves from not only floods of emails and advertisements, but from the various intrusive methods of data collection retailers employ. Another aspect that needs to be addressed is the fact that most people do not even read a website's privacy policy, and the policy is usually hard to find on the website. As an attempt to address these issues, in 2011 Senators John Kerry and John McCain initiated "The Commercial Privacy Bill of Rights Act of 2011."[188] This Bill sought to authorize the Federal Trade Commission to establish rules that require, rather than simply recommend, collectors of personally identifiable information (PII) to provide "*notice to individuals on PII collection practices and the purpose for such collection*."[189]

The Commercial Privacy Bill of Rights Act of 2011 would only apply to commercial uses of personal data, which includes data that is linkable to a specific individual.[190] This Bill establishes a set of consumer rights that "inform[s] consumers of what they should expect of companies that handle personal data."[191] However, this bill also recognizes that with an increasingly interconnected society, consumers will have to take on some responsibility to protect their own privacy.[192] Accordingly, this Bill balances these two objectives by requiring the

---

[188] Connelly, *supra* note 176.

[189] *Id.*

[190] *Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, THE WHITE HOUSE (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter *Consumer Data Privacy*].

[191] *Id.*

[192] *Id.*

content of privacy policies to include "the goals or purposes that consumers can expect to achieve by using a company's products or services, the services that the companies actually provide, the personal data exchanges that are necessary to provide these services, and whether a company's customers include children and adolescents."[193] The Bill also states that consumers have a right to individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.[194]

With regard to individual control, this Bill would require companies to provide consumers control, upfront, over the personal data the company is able to collect from the consumer, along with the use and disclosure of that data.[195] In order to accomplish this, the Bill states that companies should provide consumers with easy and accessible mechanisms that reflect the sensitivity of the data collected.[196] In addition, the Bill claims that companies should present consumers with reasonable methods of withdrawing and limiting consent to collection of personal data.[197] This is exactly the type of regulation needed to provide consumers with the option of having their personal information collected. By requiring companies to offer this choice to consumers, litigation over privacy policies would drastically decrease.

As for transparency, this Bill states that companies should clearly assert what personal data it is collecting, the purpose for which it is collected, how the data will be used, and when it

---

[193] *Id.*

[194] *Id.*

[195] *Consumer Data Privacy*, *supra* note 190, at 11.

[196] *Id.*

[197] *Id.*

will share the data with third parties.[198] Also, regarding respect for content, this Bill maintains that companies should limit its use and disclosure of personal information to purposes consistent with the context in which the data was originally disclosed.[199] This will allow consumers to make an informed decision as to whether and what type of information to allow the company to collect, which will let consumers chose how to best protect their personal information.

Next, with regard to security, this Bill proposes that companies assess "the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure."[200] This is especially important because if companies do not take safety measures with regard to privacy of consumer information, the results can be catastrophic. For example, in December 2013, hackers stole tens of millions of Target customers' credit card and personal information.[201] This resulted in millions of people having to cancel their credit cards and closely monitor their bank accounts for signs of fraud, along with a loss of faith in the Target brand.[202]

As for access and accuracy, this Bill would compel companies to use reasonable measures to ensure it maintains accurate personal data and provides consumers with access to their personal data and the opportunity to request the removal or limitation of their

[198] *Id.* at 14.

[199] *Id.* at 15.

[200] *Consumer Data Privacy*, *supra* note 190, at 19.

[201] Matthew Rocco, *Target Says Data Theft May Include 40M Cards*, FOXBUSINESS.COM (Dec. 19, 2013), http://www.foxbusiness.com/industries/2013/12/19/target-confirms-major-card-data-theft-during-thanksgiving-1487625092/.

[202] *Id.*

information.[203] This section, again, further reinforces the right of consumers to have their personal information removed from a company's database.

Concerning focused collection, this Bill would require that companies only collect the minimum amount of personal data needed to accomplish their purpose.[204] Also, once companies no longer need a consumer's personal information, the company should dispose of or de-identify it.[205] Thus, this requirement would force companies to engage in upfront decision-making about the kinds of data they need to collect to accomplish specific purposes.[206] Therefore, companies will collect no more personal data than absolutely necessary, which makes less information vulnerable to theft.

Finally, this Bill mandates the already generally accepted principle that companies should be held accountable to enforcement authorities and consumers for adhering to these principles.[207]

With regard to J.Crew's privacy policy, the company, for the most part, follows the suggestions provided in the Bill. First, as we have seen, J.Crew offers customers the option to prevent tracking and stop communications from J.Crew.[208] Also, J.Crew explicitly states the type of data it collects and why it collects such data.[209] J.Crew also states that it may share consumer information with third parties for a list of purposes.[210] As for security, J.Crew states that it takes

---

[203] *Consumer Data Privacy*, *supra* note 190, at 19.

[204] *Id.* at 21.

[205] *Id.*

[206] *Id.*

[207] *Id.*

[208] J.CREW, *supra* note 10.

[209] *Id.*

[210] *Id.*

"reasonable measures" to ensure the safety of consumer information, which is exactly what the Bill would mandate.[211] However, J.Crew does not offer any explanation for disposal or de-identification of consumer information once it is done being used by the company. Also, J.Crew's policy does not mention any accountability for adhering to the principles set forth in its privacy policy.

While this Bill was not enacted, considering the increased interest in privacy, it likely will not be long before Congress passes a similar bill, mandating accessible privacy policies, at the federal level.[212] This Bill contains provisions that are much needed to protect consumers' personal information from companies using it for inappropriate purposes or purposes for which the consumer does not intend. Going forth, the main goal of laws about privacy policies should focus on disclosure of details about the collection of consumer information, along with giving consumers the option of deciding what information the company shares and collects about them. Accordingly, in March 2012, the FTC issued a report outlining "the best practices for businesses to protect the privacy of American consumers and give them greater control over the collection and use of their personal data."[213] In addition, the FTC recommended that Congress enact "general privacy legislation, data security and breach notification legislation, and data broker legislation" in order to better protect consumer privacy.[214]

---

[211] *Id.*

[212] Commercial Privacy Bill of Rights Act of 2011, S.799, 112th Cong. (2011), *available at* https://www.govtrack.us/congress/bills/112/s799.

[213] *FTC Issues Final Comm'n Report on Protecting Consumer Privacy*, FEDERAL TRADE COMM'N (Mar. 26, 2012), http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy [hereinafter *FTC*].

[214] *Id.*

C. Recommendations for Concerned Consumers

Therefore, until Congress passes a law at the federal level, requiring all companies to provide privacy policies, the following are recommendations to consumers for best protecting their privacy. First, consumers should ask a variety of questions when confronted with requests for personal information.[215] The purpose of these questions is to limit the information that companies collect.[216] Initially, consumers need to be assertive when asked for information they feel is unnecessary to complete the transaction.[217] The questions consumers should ask include: Why is this information required?; What will be done with this information?; and, What benefit do I receive for providing the company with my personal information?[218]

Furthermore, consumers should not provide non-essential personal information unless they are content with the intended use of that information.[219] Specifically, consumers should be prudent in protecting their Social Security number.[220] While some organizations have a right to demand disclosure of your Social Security number, such as federal and state revenue departments, consumers have the right to refuse to provide it to most other businesses.[221]

---

[215] *What Personal Information Should You Give to Merchants?*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/what-personal-information-should-you-give-merchants (last visited Nov. 15, 2014) [hereinafter *What Personal Information*].

[216] *Id.*

[217] *Id.*

[218] *Id.*

[219] *Id.*

[220] *What Personal Information*, *supra* note 215.

[221] *Id.*

With regard to credit card security, federal law prohibits "merchants from printing more than the last five digits of an account number on a customer receipt."[222] Therefore, if a consumer discovers that a merchant is printing more data than necessary on receipts, this may be an indication that the merchant's personal information collection policies are lacking in security.[223] Another option, until a federal law concerning privacy policies is passed, is for consumers to contact their state and federal legislators and urge them to address the developing practice of merchants gathering consumer data for multiple purposes.[224]

CONCLUSION

This note has shown what the privacy policy of a mass retailer looks like and the ramifications that flow from each section. In addition, we have seen the different methods consumers can employ to enforce their privacy rights, while they might not altogether be successful. Also, we saw the results of when a company blatantly violates its own privacy policy. Furthermore, we looked at a bill that offered recommendations for best protecting consumer privacy, and while not enacted, provides the groundwork for future privacy laws. Finally, we looked at suggestions by the FTC for consumers to best protect their personal information from companies, until appropriate privacy laws are enacted. Therefore, until Congress enacts appropriate privacy laws, consumers must take it upon themselves to protect their personal information from unacceptable use by retailers and companies seeking to make money.

[222] *Id.*

[223] *Id.*

[224] *Id.*