The John Marshall Journal of Information Technology & Privacy Law

Volume 32 | Issue 1 Article 3

Fall 2015

The Truth Behind Data Collection and Analysis, 32 J. Marshall J. Info. Tech. & Privacy L. 33 (2015)

Morgan Hochheiser

COMMENT

THE TRUTH BEHIND DATA COLLECTION AND ANALYSIS

MORGAN HOCHHEISER*

INTRODUCTION

Retail companies have found a way to determine that a consumer is pregnant, possibly before the consumer's family knows she is pregnant.[1] Specifically, Target uses a consumer's past purchases to determine, very precisely, if she is expecting a child.[2] If this isn't a violation of personal privacy, what is?

Generally, advertising does not have to violate privacy, but in many instances, companies use personal information to increase their sales. For example, a Minneapolis father first learned of his daughter's pregnancy through print advertisements from Target.[3] He went to his local store to address the situation.[4] The father exclaimed, "[m]y daughter [is] […] still in high school, and you're sending her coupons for baby clothes and cribs?"[5] Target's "pregnancy-prediction" score targeted his daughter and began sending her coupons for items she might need during her pregnancy.[6] The father had no idea his daughter was pregnant before she received coupons in the mail.[7] Target collected and mined

---

* Morgan Hochheiser received her BA in History and Sociology from Indiana University in 2013. Currently, Morgan is pursuing her Juris Doctor at The John Marshall Law School, expected May 2016. She is the Symposium Editor for the Journal of Information Technology and Privacy Law.

1. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES SUN. MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES SUN. MAG.

personal data to capitalize on a teenager's pregnancy by offering her a "one stop shop" for all of her needs.[8]

One of Target's statisticians, Andrew Pole, identified "about 25 products that, when analyzed together, allowed him to assign each shopper a 'pregnancy prediction' score."[9] This enabled Target to "send coupons timed to very specific stages of [a shopper's] pregnancy.[10] After the incident with the Minnesota family, Pole realized that women and their families were reacting negatively to specialized "pregnancy" coupons.[11] Many women felt spied on after receiving personalized pregnancy coupons.[12] Accordingly, Target began distributing random coupons relating to pregnancy.[13] This Score threatened consumer privacy. Target's plan of adding random coupons merely obscured the problem as Target still mines consumers' data to better market its products.

Many companies use data mining and direct marketing tactics to influence customers. For example, supermarkets collect data from consumers to give them personalized coupons.[14] Retail companies market based on consumer information stored in large databases.[15] Stores also obtain information through customer loyalty cards scanned at the cash register. This Article will focus on in-store data collection and how retail companies mine consumers' personal information to increase revenue.

A majority of large corporations use third party companies to collect and analyze consumer information. A few of the largest data mining companies are Equifax, Inc., TransUnion Corp, and even LexisNexis Group.[16] Consumers may or may not know that stores collect and sell this data. Consumers swipe credit cards or scan loyalty cards without suspecting that their favorite store uses their consumer information to increase revenue. Laws exist to protect consumer privacy, yet most of the protection must come from the consumer. Privacy policies inform a

---

(Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.*

12. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES SUN. MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

13. *Id.*

14. *See generally,* Katherine Albrecht, Ed. M., *Supermarket Cards: The Tip of the RETAIL SURVEILANCE Iceberg,* 79 DENV. U. L. REV. 534 (2002).

15. Drew Hendricks, *How Businesses Can Benefit from Data Mining*, TCMNET (March 21, 2013), http://www.tmcnet.com/topics/articles/2013/03/21/331429-how-businesses-benefit-from-data-mining.htm.

16. *Opt Out List*, STOP DATA MINING ME, http://www.stopdatamining.me/opt-out-list/ (last visited Sept. 28, 2014). *See also* EQUIFAX ANALYTICAL SERVICES, http://www.equifax.com/consumer/marketinganalytics/en_us; s*ee also* TRANSUNION CORP., http://www.transunion.com/; *see also generally* LEXISNEXIS GROUP, http://www.lexisnexis.com/en-us/home.page.

consumer of her rights, but she needs to actually read and understand the policies to know how she is protected. Opt-out programs exist but consumers need to fill out forms or make phone calls to successfully opt-out of data collection.[17] The consumer should not be the only entity that actively protects her data.

Unwanted data collection and analysis injures consumers because it violates their right to privacy. The regulations in place do not properly protect consumer privacy when making in-store purchases. In order to recommend a solution to these issues, this Article will discuss how retail companies obtain consumers' personal information, what they do with such information and the negative privacy implications that stem from this process. The Article will address the following issues: (a) increase of company profits does not outweigh the privacy implications of data mining; (b) the Fourth Amendment of the United States Constitution does not fully protect consumers; (c) the current privacy laws implemented by the Federal Trade Commission ("FTC") and other administrative agencies and the lack of protections from such laws; (d) the current privacy laws enacted by various state statutes and how these laws should be universal; and (e) a proposal of regulations to protect consumer privacy that focuses on company action, not consumer action.

BACKGROUND

Data science has been around for decades and data technology is constantly evolving.[18] In recent decades, computers collect information and store it in databases when a credit or debit card is used.[19] Information collected from databases is usually analyzed through data mining. Data mining "is the exploration and analysis of large quantities of data to discover meaningful patterns and rules."[20]

Data mining companies "collect and organize information."[21] This

---

17. *See Opt Out List*, *supra* note 16 (A website where consumers can opt-out of the collection of their information).

18. *See* Gil Press, *A Very Short History of Data Science*, FORBES (Sept. 26, 2014), http://www.forbes.com/sites/gilpress/2013/05/28/a-very-short-history-of-data-science/ (describing events in 1974, when Peter Naur published a book covering contemporary data processing methods. Also describing events in 1996, when "data science" was first included as a term in the title of a conference. Further, in 1997, "the journal Data Mining and Knowledge Discovery is launched" and data mining becomes a more favored way to analyze data).

19. *See* USA EPAY, *Consumer Billing Database*, EPAY (Sept. 26, 2014, 12:40 PM), http://www.usaepay.com/custbilling.htm.

20. MICHAEL J. A. BERRY & GORDON S. LINOFF, DATA MINING TECHNIQUES 7 (Wiley Publishing Inc., 2nd ed. 2004) (explaining that data mining can be both directed and undirected; directed mining uncovers a target field whereas undirected mining attempts to find patterns without a specific target field or predefined classes).

21. *See IMS Health Inc. v. Ayotte*, 550 F.3d 42, 74 (1st Cir. 2008) (Lipez, J., dissenting) (discussing how data mining companies collected information "about doctors and

practice succeeds when large amounts of data is collected; in the case of retail stores, the use of credit or debit cards and barcode scanners "means that data is being produced and collected at unprecedented rates."[22] Data mining increases marketing potential and consequentially increase stores' profits.[23] "Customer segmentation," a type of data mining, uses consumer demographics to "tailor products, services and marketing messages to each segment."[24] Target's selection of pregnant women is an example of customer segmentation.[25]

Catalina Marketing is another large data mining company that helps companies target consumers and promote their marketing strategies through consumer data analysis.[26] Catalina's two and a half petabyte (two and a half *million* gigabytes) database of information mostly consists of consumer data extracted from the use of store loyalty cards.[27] Catalina's databases and analysis programs predict and reveal "the power of promotions, delivered through coupons, to change purchasing behavior."[28] This practice negatively impacts consumer privacy, which will be addressed later in this article.[29]

Antitrust and trade law governs consumer privacy through an administrative agency called the Federal Trade Commission ("FTC").[30] Pursuant to 15 U.S.C. § 45, the FTC must ensure that no "unfair methods of competition in or affecting commerce or deceptive acts or practices in or affecting commerce" occur, as they are unlawful.[31] The FTC developed various statutes in an attempt to enforce consumer privacy in the marketplace.[32] For example, the Fair Credit Reporting Act ("FCRA") regulates consumer reporting agencies and ensures consumer

---

their prescribing patterns, converting information gleaned from 'thousands of sources' into a commodity," sold in the pharmaceutical industry).

22. Berry, *supra* note 20 at 111.

23. Hendricks, *supra* note 15.

24. *Id.*

25. Duhigg, *supra* note 1.

26. *Insights*, CATALINA MARKETING (Sept. 27, 2014, 6:34 PM), http://www.catalinamarketing.com/insights/.

27. Doug Henschen, *Catalina Marketing Aims For The Cutting Edge of 'Big Data'*, INFORMATION WEEK (Sept. 28, 2014, 1:07 PM), http://www.informationweek.com/big-data/big-data-analytics/catalina-marketing-aims-for-the-cutting-edge-of-big-data/d/d-id/1099971.

28. *Id.*

29. *See infra* notes 62 through 65 and accompanying text.

30. *See What We Do*, FED. TRADE COMM'N (Oct. 7, 2014, 1:43 PM), http://www.ftc.gov/about-ftc/what-we-do.

31. 15 U.S.C. § 45 (2012).

32. *See* 15 U.S.C. § 6801(2012) (requiring "each financial institution [to have] an affirmative and continuing obligation to respect the privacy of its customers and protect the security and confidentiality[...]"); *see also* 5 U.S.C. §552a (2012) (requiring the federal government to prevent unauthorized disclosures of personal information).

reports are within the scope of the law.[33] Alternatively, under the Fair Debt Collection Practices Act ("FDCPA"), "third-party debt collectors are prohibited from employing deceptive or abusive conduct in the collection of consumer debts incurred for personal, family, or household purposes."[34] Those statutes are examples of FTC regulations that do not directly correspond with retail data collection but still, to some extent, protect consumers.

During a time of rapid technological change, the FTC has proposed ways to protect consumers. The following proposed three step framework addresses the collection of consumer information: "privacy by design;" "simplified choice;" and "greater transparency."[35] "Privacy by design" focuses on companies encouraging consumer privacy in their practices through data security and management; "simplified choice" allows companies to offer the choice of data collection when the consumer is ready to make the decision rather than immediately before data collection; "greater transparency" assists in creating "clearer, shorter, and more standardized" privacy policies and educating consumers about the company's data practices.[36] The FTC believes that incorporating this three-step framework into companies' policies will create the most effective practices and reinforce time-honored FTC regulations.[37]

In order to protect consumer information, legislation must distinguish protected private information from unprotected information. Although it no longer exists, House Bill 1528 explained exactly which aspects of essential "personally identifiable information" ("PII") companies must protect.[38] The Bill explained PII as:

> The combination of a first name (or initial) and last name of an individual, whether given at birth or time of adoption, or resulting from a lawful change of name; (ii) the postal address of a physical place of residence of such individual; (iii) an e-mail address of such individual; (iv) a telephone number or mobile device number dedicated to contacting such individual at any place other than the individual's place of work; (v) a social security number or other Federal or State govern-

---

33. *Trans Union Corp v. FTC*, 245 F.3d 809, 811 (D.C. Cir. 2001).

34. *Fair Debt Collection Practices Act,* FED. TRADE COMM'N, http://www.ftc.gov/enforcement/statutes/fair-debt-collection-practices-act (last visited Nov. 6th, 2014).

35. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FED. TRADE COMM'N (Dec. 2010), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

36. *Id.*

37. *See id.* at 6, 7, 10 (giving examples of FTC approaches include privacy notice and a harm-based model targeted practice to protect against identity theft, spam, unwanted telemarketing).

38. H.R. 1528, 112TH CONG. § (3) (8) (A) (2011).

> ment issued identification number issued to such individual; or (vi) the complete account number of a credit or debit card issued to such individual [...] [and] (i) a birth date, the number of a certificate of birth or adoption, or a place of birth; or (ii) an electronic address, including an IP address.[39]

Bill 1528 further proposes that a company must notify a consumer when it will use PII, particularly for purposes unrelated to the transaction.[40] Bill 1528 allowed a consumer to prohibit a company from selling their PII until they retract the prohibition, or after five years, whichever occurs first; confirmation of a company's consumer protection occurs when the consumer knows they can preclude the company from collecting PII.[41]

More recently, in 2012 the White House, under the Barack Obama administration, proposed a Consumer Privacy Bill of Rights.[42] These Bill of Rights' principles mirror those proposed by the FTC and include individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability, each of which focus on consumers rather than companies.[43] Individual control allows consumers to control who collects their data; transparency allows consumers to easily understand privacy practices; respect for context assumes consumers will know that companies have and will use their personal data in the same context that consumers provide it; security provides an accountable handling of consumer data; focused collection enables consumers to limit what personal data is collected; and accountability ensures that companies handle consumer data consistent with this Bill of Rights.[44] Both the proposed FTC framework and President Obama's proposed Consumer Privacy Bill of Rights seek to protect personal data.[45] Although the government cannot enforce the Consumer Privacy Bill of Rights, it provides a decent example of what an enforceable law should look like. The primary concern is how to enforce consumer privacy proposals.

The FTC used company stakeholders to address consumer data issues and to implement the changes themselves.[46] A stakeholder is "someone who has an interest [...] in a business [...] though not neces-

---

39. *Id.*

40. H.R. 1528, 112TH CONG. § (6) (A) (2011) (unrelated uses of PII include advertisements, coupons, other promotions, etc.).

41. *Id.*

42. PRESIDENT BARACK OBAMA, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 1 (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

43. *Id.*

44. *Id.*

45. *Protecting Consumer Data*, *supra* note 35 at 44; S*ee also* Obama, *supra* note 42 at 1.

46. *Protecting Consumer Data*, *supra* note 35 at 44.

sarily as an owner," or "a person who has an interest or concern (not necessarily financial) in the success or failure of an organization."[47] The FTC's variety of stakeholders includes representatives from the industry, government officials, advocates, and other "interested parties."[48] President Obama also developed an implementation code that included stakeholders.[49] An analysis of current laws and implementation practices will be addressed later in this Article.

Both the FTC and White House proposals overlook the issue of retail companies and third parties selling consumer data. While Bill 1528 addressed this issue, many consumers do not "opt-out" of data collection or preclude companies from selling their PII.[50] Many opt-out and selling regulations exist in state statutes or common law.[51] Many state laws protect consumers from unauthorized disclosure of PII but vary in the amount of protection afforded to consumers.[52] Many courts have upheld these state laws.[53]

Another privacy implication comes from the Fourth Amendment. The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]"[54] The Supreme Court debated the concept of the "Third-Party Doctrine" and its relationship to the Fourth Amendment.[55] According to the Court, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[56] Unfortunately for consumers, voluntarily giving away PII has become an everyday standard.[57] The implications of the Third-Party Doctrine will be

---

47. BLACK'S LAW DICTIONARY 1623 (10th ed. 2014).

48. *Protecting Consumer Data*, *supra* note 35 at 2.

49. *Protecting Consumer Data*, *supra* note 35 at 23.

50. *See* H.R. 1528, 112th Cong. § (6)(A)(2); *see also* Jeff Sovern, *Opting In, Opting Out, Or No Options At All: The Fight For Control Of Personal Information,* 74 Wash. L. Rev. 1033, 1033 (1999); s*ee also* Omer Tene*, The Second Wave of Global Privacy Protection: Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws,* 74 OHIO ST. L.J. 1217, 1246 (2013).

51. *See* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures,* 11 NW. J. TECH. & INTELL. PROP.321, 338 (2013) (discussing opt-in and opt-out scenarios for third-party disclosures).

52. *See California's "Shine the Light" Law Goes into Effect Jan. 1, 2005*, PRIVACY RIGHTS CLEARINGHOUSE (Dec. 29, 2004), http://www.privacyrights.org/ar/SB27Release.htm; *see also* VA. CODE ANN. §59.1-442 (2014).

53. *See Tyler v. Michaels Stores, Inc.*, 464 Mass. 492 (2013).

54. U.S. CONST. amend. IV.

55. RICHARD M. Thompson II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 12 (2014).

56. *Id.*

57. Kashmir Hill, *Federal Judge and His Very Famous Law Clerk Say The Fourth Amendment 'Is All But Obsolete' Thanks To Safeway Club Card, Amazon and Google*, FORBES (June 28, 2011 at 2:41 PM),

examined later in this Article.

ANALYSIS

After an in depth look at the issues surrounding data collection and the laws and regulations that should be governing it, this Article will propose regulations that will better protect consumers from the negative impacts of companies' collection and analysis of PII.

I. DATA MINING CREATES MORE PROBLEMS THAN IT SOLVES.

a. In Balancing The Benefits And Detriments In Data Mining, The Detriments Greatly Outweigh The Benefits And Therefore, There Must Be Stricter Data Mining Laws.

The process of data mining has both benefits and detriments. There are benefits to the company, which produce detriments to the consumer who provides the information. The benefits of data mining include an increase in marketing, an increase in use of resources and a better understanding of consumers; all of these benefits produce an increase in sales.[58] The impact data mining has on consumer privacy should concern all consumers. The primary benefit of data mining is a company's ability to increase profits.[59] Data mining allows companies to "collect and organize information" and also to "tailor products, services and marketing messages to each [consumer] segment."[60] As data mining increases marketing potential, it also increases a store's profits.[61] Understanding consumer feedback allows a company to give the consumer exactly what it desires and therefore seize more profit from that person. While companies strive to increase profits, they must determine if this increase is worth sacrificing consumer privacy. The benefit of data mining may be invaluable to a store, but consumers may not want to spend money at a store that compromises their privacy.

The previously discussed Target example shows how consumers disapprove of data mining, as many have had negative responses to Target's directed marketing campaign.[62] A second detriment occurs

---

http://www.forbes.com/sites/kashmirhill/2011/06/28/federal-judge-and-his-very-famous-law-clerk-say-the-fourth-amendment-is-all-but-obsolete-thanks-to-safeway-club-card-amazon-and-google/.

58. Hendricks, *supra* note 15.

59. *Id.*

60. Berry, *supra* note 20 at 597; *see also Ayotte*, 550 F.3d at 74 (discussing how data mining companies collected information "about doctors and their prescribing patterns, converting information gleaned from 'thousands of sources' into a commodity," sold in the pharmaceutical industry).

61. Hendricks, *supra* note 15.

62. Duhigg, *supra* note 1.

when companies reach out to consumers who do not want to be contacted. The Target "pregnancy-prediction model" is a great example of this.[63] Another example comes from *Tyler v. Michaels Stores, Inc.*, in which the plaintiff consumers filed a class action because the consumers received "unsolicited and unwanted marketing material from Michaels."[64] The Court held that undesired marketing injures the consumer and violates state law.[65] Thus, any time a retailer mails out unwanted advertisements, it harms current and potential consumers.

b. Fourth Amendment Issues Are Raised When Discussing Privacy And Therefore New Data Collection Laws Must Be Created As The Fourth Amendment Does Not Fully Protect Consumers.

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]"[66] This Amendment should protect citizens from having their data collected unknowingly, without probable cause, or without a warrant. Many articles have been written on the so-called "death of the Fourth Amendment."[67]

The founding fathers did not have access to electronic cash registers, cell phones, computers, and other electronic devices when they ratified the Constitution. Today, these objects infiltrate consumers' lives and affect privacy rights. During the past few decades, courts have decided cases regarding data collection and its Fourth Amendment implications.[68]

When ruling on *Katz v. United States* in 1967, the Supreme Court debated the concept of a "Third-Party Doctrine."[69] According to the Court, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[70] *Katz* also held that a per-

---

63. *Id.*

64. *Tyler*, 464 Mass. at 503 (2013), *See infra* notes 122 to 123 and accompanying text.

65. *See Tyler* at 503 (holding that "sending the customer unwanted marketing materials or by selling the information for a profit, the merchant has caused the consumer an injury[.]").

66. U.S. CONST. amend. IV.

67. Hill, *supra* note 57; s*ee also* Thompson II, *supra* note 55 at 12; *see also* Chris Weigant, *Friday Talking Points—Rest in Peace, Fourth Amendment*, HUFFINGTON POST (Aug. 7th, 2013, 5:12 AM), http://www.huffingtonpost.com/chris-weigant/friday-talking-points_b_3405819.html.

68. *See United States v. Jones*, 132 S.Ct. 945 (2012)(affirming the decision of the United States Court of Appeals for the District of Columbia Circuit reversing Defendant's conviction of drug conspiracy with "evidence obtained through a global-positioning-system (GPS) device."); *see also* City of Ontario v. Quon, 560 U.S. 746, 130 S.Ct. 2619 (2010); s*ee also* Ex Parte Jackson, 96 U.S. 727, 733 (1877); *see also* Thompson II, *supra* note 55 at 12.

69. Thompson II, *supra* note 55 at 12.

70. *Smith v. Md.*, 442 U.S. 735, 743-44, (1979); *see also* Thompson II, *supra* note 55

son may be protected under the Fourth Amendment if they desire to keep something private, regardless of whether it is in the public sector.[71] Accordingly, if a consumer voluntarily provides PII to a company, then that consumer does not have a Fourth Amendment claim.

In *Ex Parte Jackson*, the Supreme Court determined whether the Fourth Amendment protected postal mail.[72] Petitioner was jailed for "knowingly and unlawfully depositing in the mail [...] a circular concerning a lottery offering prizes."[73] The Supreme Court held that the Fourth Amendment protects letters and other sealed mail, but not the "printed matter" on the outside of the envelope.[74] Applying this holding, a consumer's written address for a store promotion is not protected by the Fourth Amendment, as it is synonymous with the "printed matter" in *Ex Parte Jackson*. Although highly debated, companies are protected under the Third-Party Doctrine when they obtain consumer information without consent.

The "death" of the Fourth Amendment stemmed from the Third-Party Doctrine.[75] Individuals giving away PII relinquish Fourth Amendment protection as to that information.[76] An intentional swipe of a credit card at Target, for example, voluntarily gives away private information, and the Third-Party Doctrine trumps the Fourth Amendment. Today, many citizens do not even know what the Fourth Amendment protects.[77]

While the Fourth Amendment may not directly protect consumer privacy, consumers should have some right to protection.[78] Whether or not there is a Fourth Amendment violation needs to be established on a case-by-case basis. Overall, data collection influences Fourth Amendment protections and should be taken into account when proposing new consumer privacy regulations.

---

at 12.

71. *See Katz v. United States*, 389 U.S. 347, 351 (1967) *abrogated in part as stated in United States v. Figueroa-Cruz*, 914 F. Supp. 2d 1250 (11th Cir. 2012) *and superseded by statute as stated in United States v. Koyomejian*, 946 F.2d 1450 (9th Cir. 1991).

72. *Ex Parte Jackson*, 96 U.S. 727.

73. *Id.*

74. *Id* at 733; Thompson II, *supra* note 55 at 12.

75. Thompson II, *supra* note 55 at 12.

76. Hill, *supra* note 57.

77. *See generally* Stephanie Grace & Alex Kozinski, *Remember what the Fourth Amendment protects? No Just as well,* AXIS OF LOGIC (June 22, 2011), http://axisoflogic.com/artman/publish/Article_63269.shtml.

78. *See infra* notes 38 to 39 and accompanying text.

c. Companies Use Various Methods of Direct Marketing To Consumers And Therefore The Laws Must Incorporate Other Forms Of Data Collection And Use.

Many companies that use data analysis to increase effective marketing also take part in directed marketing to retain customers. Other forms of marketing include loyalty cards and GPS tracking. Store loyalty cards have been around for more than twenty years, making their debut in the early 1990's.[79] Loyalty cards give shoppers discounts on purchased items with one catch: shoppers end up trading personal information for loyalty cards to obtain access to sales.[80] Just as shoppers may not know that stores analyze their data, shoppers probably do not realize that loyalty cards track their data.[81] Even shoppers who evade data collection by paying with cash give away information when signing up for a loyalty card. Shoppers believe loyalty cards provide a good bargain, but fail to consider negative privacy implications such as unwanted advertisements or security breaches. For example, Jewel Osco ended its loyalty card program and enacted price drops for the entire store.[82] Now, Jewel Osco shoppers can reap the benefits of having access to loyalty card prices, but without the privacy implications that come along with one.

Another aid to in-store marketing is GPS tracking. In particular, one upscale store used its Wi-Fi system to track shoppers.[83] Nordstrom began using a system called Euclid to track its consumers' cell phones while they shopped.[84] Nordstrom used Euclid to determine where shoppers lingered and to "get a better sense of customer foot traffic."[85] After obtaining this information, Nordstrom can modify its marketing strategies to conform to what shoppers want by tracking the time they spend at certain displays.

Euclid's CEO, Will Smith, stated that Euclid increases revenue by helping clients "match the supply of sales people with the demand for their services" by "measur[ing] how long people stay inside the store."[86] Euclid also "keep[s] track of the proportion of people who walk by the store window" in addition to those who walk into the store.[87] Euclid's

79. Albrecht, *supra* note 14.

80. *Id.* at 535.

81. *Id.* at 536.

82. Allison Sperling, *Card Free Savings for All Shoppers!*, JEWEL OSCO (Jun. 26th, 2013), http://www.jewelosco.com/2013/06/card-free-savings/.

83. Peter Cohan, *How Nordstrom Uses WiFi To Spy On Shoppers*, FORBES (May 9th, 2013 at 8:23 AM), http://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers/.

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

creators kept consumer privacy a priority when creating the program.[88] Posted signs in stores tell shoppers that they may opt out of tracking by turning off their cell phones.[89] Additionally, Euclid does not extract any PII from tracking cell phones.[90] Even with these safeguards, the fact that a retail store can track a consumer's phone for marketing purposes intrudes on privacy.[91]

The use of credit cards, debit cards, loyalty cards, and cell phone tracking are just a few examples of how stores collect consumer data.[92] Stores analyze the collected data to better market their products to consumers. Some stores change displays and others send out consumer-specific advertisements and coupons. While this increases store revenue, it impacts consumer privacy, as the data sits in a database waiting to be used or possibly sold to an unknown third-party. For example, consumer data that is stored in a database can be breached and stolen by hackers, as evidenced by the Target data breach in 2013, which affected nearly 70 million customers.[93] These data breaches allow hackers to further impersonate and lure victims "to give up more sensitive information."[94] Hackers stole approximately "40 million customers' credit and debit card information" during the Target data breach and approximately 30 million more customers had their name, address and phone number stolen.[95] This breach could have been less tragic if consumer data was not stored in a database. More recently the match-making website, Ashley Madison, was the victim of a data breach. The hackers publicly disclosed "data from about 31 million accounts" and included "a lot of sensitive information about the people (mostly men) who used the site, including email addresses, cities of residency, and sexual prefer-

---

88. *Id.*

89. Peter Cohan, *How Nordstrom Uses WiFi To Spy On Shoppers,* FORBES (May 9th, 2013 at 8:23 AM), http://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers/.

90. *Id.*

91. *See* Christopher Matthews, *Future of Retail: How Companies Can Employ Big Data to Create a Better Shopping Experience*, TIME (Aug. 31st, 2012), http://business.time.com/2012/08/31/future-of-retail-how-companies-can-employ-big-data-to-create-a-better-shopping-experience/print/ (discussing the privacy impacts on "tracking users on smartphones" and how those practices have "made many in the public uncomfortable").

92. Data can also be collected through written or verbal surveys, coupon use, online tracking and more.

93. Jia Lynn Yang and Amrita Jayakumar, *Target says up to 70 million more customers were hit by December data breach*, WASHINGTON POST (Jan. 10, 2014), http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html.

94. *Id.*

95. *Id.*

ences."[96] Ashley Madison offered users a "delete forever service that really did not delete the data" which "shows that the treatment and management of data is a real concern."[97] Users of websites such as Ashley Madison and consumers of stores such as Target expect that their PII will be safe. While technology has benefits and detriments, the consequence of infringing on a consumer's privacy does not outweigh the benefit of raising companies' revenue. The FTC and Other Administrative Agencies must be tougher in enforcing consumer protection laws.

d. The FTC's Proposed And Enacted Laws Relating To Privacy Should Be Used As A Foundation Of A New Consumer Privacy Law.

As mentioned, the FTC is a government administrative agency that is governed by antitrust and trade law.[98] The FTC regulates privacy and brings suit against companies who engage in "unfair methods of competition in or affecting commerce or deceptive acts or practices in or affecting commerce."[99] The FTC has filed suits against numerous companies for failing to follow the U.S. Code, but it has not filed any lawsuits against companies for in-store data collection practices.[100]

The FTC proposed a framework to help further protect consumers from having their PII disclosed without permission.[101] During roundtable discussions of the proposed regulation, the FTC heard from expert panelists describing the massive amounts of data collected each day and the need to regulate it.[102] The framework consists of three steps: "privacy by design;" "simplified choice;" and "greater transparency."[103] Along with those three steps, the FTC focuses on education for

---

96. Dina Spector, *A 'cheating' husband reveals what it feels like to be exposed in the Ashley Madison hack,* BUSINESS INSIDER (Sep. 2, 2015, 5:29AM), http://www.businessinsider.com/what-it-feels-like-to-be-exposed-in-ashley-madison-data-breach-2015-9?r=UK&IR=T.

97. Russell Walker, *Serious Big Data Lessons from the Ashley Madison Data Breach,* LINKEDIN, (Jul 30, 2015), https://www.linkedin.com/pulse/serious-big-data-lessons-from-ashley-madison-breach-russell-walker.

98. *See What We Do*, *supra* note 30.

99. 15 U.S.C. § 45.

100. *See FTC Files Complaint Against Wyndham Hotels for Failure to Protect Consumer's Personal Information*, FED. TRADE COMM'N (June 26, 2012) (hereinafter *Wyndham* Hotels)http://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect; *see also FTC Charges Operators of "Jerk.com" Website With Deceiving Consumers*, FED. TRADE COMM'N (Apr. 17, 2014) http://www.ftc.gov/news-events/press-releases/2014/04/ftc-charges-operators-jerkcom-website-deceiving-consumers (discussing that the majority of suits brought by the FTC relate to online data collection and data breaches).

101. *Protecting Consumer Data*, *supra* note 35 at 43.

102. *Id.* at C-1.

103. *See id.* at ix (describing "Privacy by design" which focuses on companies encouraging consumer privacy in their practices in ways such as data security and management;

business and consumers.[104] The FTC created websites to help consumers learn about various privacy matters including online security protection.[105]

The FTC also protects consumers under other statutes concerning fair credit, fair debt, protecting financial transactions, and protecting health information.[106] These statutes provide for the "administrative responsibilities" of the FTC; although they are not data centric, they provide examples and descriptions of essentials that should be included in an FTC regulation of data collection.[107] An important distinction between what data may or may not be collected appears in the Fair Credit Reporting Act ("FCRA").[108] The FCRA regulates consumer reporting agencies and ensures that consumer reports are within the scope of the law.[109] The FCRA describes the furnishing of a consumer report and defines a consumer report as:

> any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness [creditworthiness], credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for—
>
> (A) Credit or insurance to be used primarily for personal, family, or household purposes;
>
> (B) Employment purposes; or
>
> (C) Any other purpose authorized under section 604 [15 USCS § 1681b].[110]

The FCRA protected consumers in 2001 when the FTC sued a consumer reporting agency, TransUnion Corp., for selling "lists of names and addresses to target marketers."[111] The Court held that the lists sold by TransUnion Corp. were categorized as consumer reports under 15 U.S.C. §1681a and therefore could not lawfully be sold to target mar-

---

"Simplified choice" which allows companies to offer the choice of data collection at a point in time when the consumer is ready to make the decision as opposed to prior to data collection; and "Greater transparency" which assists in creating "clearer, shorter and more standardized" privacy policies and educating consumers regarding the company's data practices).

104. *Id.* at 78.

105. *Id.* at 13-14.

106. *Statues Enforced or Administered by the Commission*, FED. TRADE COMM'N, http://www.ftc.gov/enforcement/statutes?title=&&page=1 (last visited Oct. 18th, 2014).

107. *Id.*

108. 15 U.S.C. § 1681 (2012).

109. *Trans Union*, 245 F.3d 809.

110. 15 U.S.C. § 1681(a).

111. *Trans Union* at 811.

keters.[112] By categorizing a list of names and addresses as a "consumer report," the court created an inference that all databases that (a) include personal information and (b) are sold to data mining companies, should be a violation of the FCRA.[113] Therefore, selling consumer names and addresses to third parties should be illegal under the FCRA and the FTC should take better steps to regulate FCRA violations.

Although the FTC has been regulating consumer privacy for decades, it lacks adequate direct regulation in the collecting, selling, and mining of consumer data. The proposed three-step framework would help overcome this gap in regulation. Strengthening FTC regulations on the collecting, selling, and mining of consumer data will reinforce consumer privacy rights.

e. The Consumer Financial Protection Bureau Must Continue To Support Consumer Protection And Laws Must Be Enacted To Ensure Such Protection.

Along with the FTC, the Consumer Financial Protection Bureau ("CFPB") is an administrative agency that assists consumers in a financial capacity.[114] Congress established the CFPB principally to "write rules, supervise companies, and enforce federal consumer financial protection laws."[115] In recent years, the CFPB has not fulfilled its oversight duties to promote consumer privacy. The CFPB abused its power and collected financial data connected to 600 million credit card accounts.[116] The CFPB should protect consumers but instead "lacks written procedures for protecting data and needs to beef up its information security practices," according to the Government Accountability Office.[117]

The CFPB recently demanded consumer data from banks, which posed a problem for the banks since it affects the privacy of their consumers.[118] The CFPB gave no details as to why it collected the data and how it would store it. Now consumers must worry about what retailers,

---

112. *Id.* at 818-19.

113. *See generally id.*

114. *About Us*, CONSUMER FINANCIAL PROTECTION BUREAU, http://www.consumerfinance.gov/the-bureau/ (last visited Oct. 18th, 2014).

115. *Id.* (describing how the CFBP also educates consumers and studies data to "better understand consumers, financial services providers, and consumer financial markets").

116. Natalie Rutledge, *CFPB Keeps Data On Nearly 600 Million Credit Card Accounts*, LOWCARDS (Oct. 8th, 2014), http://www.lowcards.com/cfpb-data-600-million-credit-card-accounts-27978.

117. Alan Zibel, *GOA: CFPB Should Take Steps to Protect Consumer Data Collected From Banks,* THE WALL STREET JOURNAL (Sept. 22nd, 2014 6:21 PM), http://online.wsj.com/articles/gao-cfpb-should-take-steps-to-protect-consumer-data-collected-from-banks-1411424490.

118. *Id.*

third parties, and protection agencies will do with their personal information. Regulations must be enforced or the CFPB must be penalized to deter deceptive practices.

f. The Executive Branch Wants Consumer Protection And Therefore Proposed Guidelines Should Be Taken Into Account For New Consumer Protection Laws.

President Barack Obama proposed the Consumer Privacy Bill of Rights to act as guidelines for data collection and consumer privacy. The Privacy Bill of Rights includes individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability, each of which focuses on consumers rather than companies.[119] The focus on consumers offers more control on what information companies can collect. Yet, by focusing on consumers, enforcing the Bill of Rights is nearly impossible. For example, if the Bill of Rights regulated companies, then the companies would be reprimanded for not following the guidelines. But if a consumer does not follow the Bill of Rights, how can she be reprimanded? Focusing on consumer action will strengthen privacy protection but consumers must be active on their own to ensure maximum protection.

A consumer has the choice to follow the Privacy Bill of Rights. If a consumer chooses not to limit the information she gives to a company or does not ask where her data goes, she cannot protest if a company sells her data to a third-party. The Privacy Bill of Rights forces consumers to take action to ensure her PII stays protected. If a consumer accidentally (or purposefully) does not keep a tight grasp on her PII, the Privacy Bill of Rights does not punish the companies who collect such information. Thus, the Privacy Bill of Rights truly does not protect consumers who do not actively protect their private data.

II. STATE STATUTES AND REGULATIONS SHOULD BE COMBINED INTO A UNIFORM FEDERAL LAW IN ORDER TO BEST PROTECT CONSUMER PRIVACY.

In addition to federal guidelines, including the FTC, CFPB, and President Obama's proposal, many states have their own statutes cover-

119. *See* Obama, *supra* note 42 (describing how individual control allows consumers to control who collects their data; transparency allows consumers to easily understand privacy practices; respect for context assumes consumers will know that companies have and will use their personal data in the same context that consumers provide it; security allows consumers to have an accountable handling of their data; access and accuracy allows for consumers to appropriately collect personal data; focused collection allows for consumers to limit what personal data is collected; and accountability allows consumers to have their data handled in a way consistent with the Bill of Rights).

ing consumer privacy.[120] These statutes range from prohibiting the collection of data to prohibiting the sale of consumer PII.[121] State laws can be extremely useful to see the various protections consumers have and to guide federal consumer privacy law. The following state laws give a condensed overview of various state laws protecting consumer privacy.

In *Tyler v. Michaels Stores, Inc.,* Massachusetts law governed and prohibited a store from requiring "that a credit card holder write personal identification information, not required by the credit card issuer, on the credit card transaction form. Personal identification information shall include, but shall not be limited to, a credit card holder's address or telephone number."[122] The Court further stated that a violation of this Massachusetts statute would be an "unfair and deceptive trade practice" and thus would violate FTC rules and regulations.[123] The Massachusetts statute cited in *Tyler v. Michaels Stores, Inc.,* focuses on what data a store is prohibited from collecting when a consumer uses a credit card to pay for her purchase.

In 2005, California enacted the "Shine the Light" Law, which provides consumers with notice when a business sells consumer information to a third-party.[124] This Law ensures that consumers, when requested, will be notified with whom businesses share PII with.[125] Businesses that have already established opt-out provisions are exempt from this law.[126] "Shine the Light" provides damages of up to $3,000 if a business intentionally does not comply with a consumer request.[127] This and other similar laws give consumers an opportunity to learn what third parties have their information and determine if they desire to shop at that business.[128] For example, under this law, Target would have to disclose the third parties who collect consumer information and consumers may decide to shop elsewhere.

Connecticut requires businesses that collect Social Security numbers to publically display their privacy policy.[129] The Law requires the public display of the privacy policy to be in more places than merely "posting on [it] an Internet web page" and the "policy shall: (1) protect the confidentiality of Social Security Numbers, (2) prohibit unlawful

---

120. *Shine the Light, supra* note 52; *see also* VA. CODE ANN. §59.1-442; *see also* CONN. GEN. STAT. §42-471(b) (2009).

121. *Shine the Light, supra* note 52; *see also* VA. CODE ANN. §59.1-442 ; *see also* CONN. GEN. STAT. §42-471(b).

122. *Tyler* at 495; *see also* ALM GL Ch. 93, § 105 (1991).

123. *Tyler* at 495.

124. Cal. Civ. Code § 1798.83 (2005); *see also Shine the Light, supra* note 52.

125. *Shine the Light, supra* note 52.

126. *Id.*; *see* i*nfra* notes 139 through 141 and accompanying text.

127. *Shine the Light, supra* note 52.

128. *Id.*

129. CONN. GEN. STAT. §42-471(b).

disclosure of Social Security numbers, and (3) limit access to Social Security numbers."[130] While a store, such as Target, is unlikely to require a consumer's Social Security number at checkout, demanding businesses to publically disclose the collection of Social Security numbers allows for greater consumer protection. Yet, the Law gives businesses a loophole to collect Social Security numbers when giving public notice. However, under this Law, consumers have the ability to choose stores that comply with their privacy protection needs, which ultimately increases privacy protection.

Virginia's Personal Information Privacy Act prohibits merchants who do not give the consumer notice from selling PII to third-parties collected during the sale.[131] Under this Act, notice can be "any…reasonable method," including posting a sign.[132] A merchant "means any person or entity engaged in the sale of goods from a fixed retail location in Virginia."[133] The Act further prohibits merchants from selling "any information gathered solely as the result of any customer payment by personal check, credit card, or where the merchant records the customer's driver's license number."[134] The Virginia Code protects consumers from having their information sold to a third-party but similar to the Connecticut law, gives the merchant a loophole, thus undermining consumer protection. Once again, consumers have a choice to shop at stores that may disclose PII.

These various state laws are examples of what should be included in a Federal consumer protection act. Incorporating state regulations into one uniform law will create an effective defense to unfair data collection, mining and the selling of consumer information.

III. PROPOSAL

In order to eradicate the privacy issues with retail data collection and consumer privacy, a statute or regulation must include a number of elements. These elements come from the FTC proposed regulations, the White House's Privacy Bill of Rights, numerous state statutes and other concepts discussed in this Article. The best way to protect consumer rights is to ensure that the companies follow the regulations. In order to do so, the following elements must be included: (a) rules based on company action; (b) penalties for selling PII to third-parties strictly for marketing purposes; (c) publicity of how and what PII is collected; and (d) modernization of the Third-Party Doctrine created by the Supreme Court.

---

130. *Id.*
131. VA. CODE ANN. §59.1-442.
132. *Id.*
133. *Id.*
134. *Id.*

A. CONSUMER PRIVACY REGULATIONS

i. Company Based Regulations

Congress charged the FTC with promoting fair trade practices and disciplining companies that do not follow the regulations.[135] However, the FTC must better enforce these regulations. As mentioned, the FTC sued numerous financial institutions and online retailers who violated these regulations, yet the FTC has not taken a strong stance against any in-store consumer privacy violations.[136] Company-based regulations will allow the FTC to target specific companies who violate the regulations and discipline them. It is more difficult for the FTC to enforce rules based on consumer action. Such laws would penalize consumers that do not actively protect their privacy, without adequately protecting consumer privacy. A company-based regulation holds businesses personally accountable for consumer protection and allows for the passive protection of rights by the consumer. Privacy protection should be a right, not a privilege.

In the financial atmosphere, the CFPB must also ensure consumer protection. Regulations created for banks and other financial institutions must be controlled. If the CFPB continues to violate consumer privacy by collecting and maintaining over a 500 million consumers' information, Congress must step in and reprimand the CFPB.[137] By doing so, consumers in the financial atmosphere will be better protected. Reprimanding the CFPB will again allow for passive protection of rights by the consumers as the protection would be company based. The CFPB demonstrates to the FTC the wrong approach for consumer protection.

ii. Notice, Permission And Third-Party Disclosure

Do companies really need all of the information they collect? While the FTC cannot sue a company for marketing, companies should reevaluate exactly what information is necessary to increase revenue without encroaching on consumer privacy. After reevaluation, companies should give notice of marketing techniques and describe what information could be collected. Target, for example, should post in-store signs to tell consumers that their personal information may be collected upon payment with a credit or debit card. The notice should also include what information will be collected and for what purpose. Collection of a social security number upon checkout is usually unnecessary, while name and address may be more prevalent to data mining or marketing analysis. This notice should also include that the company's analysts or

135. 15 U.S.C. § 45.

136. *See Wyndham Hotels supra* note 100; *Jerk.com*, *supra* note 100.

137. Rutledge, *supra* note 116.

third-parties may analyze the gathered data and for what purpose they intend on using the data.[138]

The last aspect of notice serves to remind consumers about the collection of PII immediately before completing the purchase. This task may seem like a burden and a waste of time, but each time a consumer checks out at Target, for example, the cashier asks if they want to sign up for a Target credit card. It would be an easy addition to remind the consumer that their PII may be collected. After reminding the consumer about the store's data collection policy, a second step that companies should implement is to ask the consumer if they will allow the collection of their information.

By creating opt-in programs, instead of opt-out programs, the burden switches to the company to protect the consumer. Further, more consumers are likely to use the opt-in program if the company asks them directly.[139] Opt-out programs do not work as well as opt-in programs because consumers rarely take the necessary steps to opt-out.[140] Some consumers put their names on opt-out lists, while others "pa[y] fees to services which purport to reduce or eliminate commercial solicitations."[141] For this step to work properly, the company must not require any additional information for credit or debit card use. If the company requires such information, it must ensure that it will only be used for transaction and not for future use. Consumers should also have the option to opt-out at a later date. Consumer choice directly corresponds with the FTC's proposed framework of a "simplified choice."[142]

Third, companies must disclose which third-parties may receive consumer information, if the consumer opts-in for data collection. The company should also disclose specifically what information it will give to the third-party company. By producing a list of companies that may receive PII, the consumer has a better understanding of exactly who has access to their information. In a perfectly protected data environment, a consumer would have the choice to decline giving third-parties PII and also could opt-in to have the PII used for advertisements and coupons from the company. This step corresponds with President Obama's Privacy Bill of Rights; specifically, the individual control section, which allows consumers to control who collects their data. Also, the context section assumes consumers will know that companies have and will use their personal data in the same context that consumers provide it.[143]

Together, the following steps comprise the notice portion of the

---

138. Examples of why data could be used include marketing purposes, advertisements, coupons, etc.

139. *See* Sovern, *supra* note 50 at 1033; *see also* Tene, *supra* note 50 at 1246.

140. *See* Sovern, *supra* note 50 at 1033; *see also* Tene, *supra* note 50 at 1246.

141. Sovern, *supra* note 50 at 1068.

142. *Protecting Consumer Data*, *supra* note 35 at v-viii.

143. Obama, *supra* note 42 at 1.

proposed regulation. First, companies must give notice of their marketing techniques and describe what information could be collected. Second, companies should ask the consumer if they opt-in to data collection. Lastly, companies must disclose which third-parties may receive consumer information, if the consumer opts-in to data collection. The next section of the proposed regulation focuses on selling consumer data.

iii. Consumer Data Should Not Be Sold.

Companies will often sell the collected data to data mining companies for analysis even though this practice exploits consumer privacy. While the benefits of data mining have merit, companies should not make money by violating consumer privacy.[144] In practice, each data mining company should have companies as clients. For example, Target would pay a data mining company to analyze the data it receives, which would be a simple payment for work product.[145] California's "Shine the Light" law and Virginia's Personal Information Privacy Act already require notice of third-party involvement and ban the sale of consumer information without such notice.[146] These two regulations force companies to take action, conforming to the above, and also prohibit the sale of data in certain circumstances.[147] But in order to fully protect consumer privacy, data simply should not be sold.

Selling data exploits a consumer and therefore is against public policy. The public needs to trust businesses and the government, but if businesses sell private information and the government allows it, the public has no one to trust with their PII. In order to have a free market with buyers and sellers, there must be trust. A consumer needs to trust that the business will not collect PII without their consent; the business must trust that the consumer trusts the business practices enough to continue purchasing its products. If a business sold consumer information to undisclosed third-parties, the consumer would be less inclined to trust the business and more likely to refrain from purchasing the business's products. Exploiting consumer privacy to raise revenue violates trust and therefore tarnishes the marketplace.

iv. Fines and Other Penalties.

A fine should be imposed when companies collect consumer data without consumer permission or notice. The fine should be a fixed fee per violation (e.g. $1,000.00 per consumer). If PII such as social security

144. *See infra* notes 58 through 61 and accompanying text.
145. Henschen, *supra* note 27.
146. *Shine the Light, supra* note 52; *see also* VA. CODE ANN. §59.1-442.
147. *Shine the Light, supra* note 52; *see also* VA. CODE ANN. §59.1-442.

numbers are collected, then the fine should increase as social security numbers need greater protection. If a merchant sells consumer data for marketing purposes, a fine should also be imposed. In that case, the fine should be a combination of a fixed fine in addition to an adjustable fine depending on the personal information sold (e.g. $1,000.00 for consumer name plus $1,000.00 for consumer address, etc.). Imposing fines on merchants will deter them from violating the regulations and further protect consumer data.

The FTC should also increase the number of suits it files against merchants. As seen, the FTC often files suit against online retailers when data breaches or fraud is present. The FTC should also file suit against merchants who collect or sell data without permission. If the FTC increases its enforcement, consumers will be more protected.

B. FOURTH AMENDMENT THIRD-PARTY DOCTRINE

The Third-Party Doctrine "[leaves] unprotected anything a person knowingly exposes to the public," and should be overturned.[148] This Doctrine has been highly criticized and should be modernized to reflect the need for more efficient protection.[149] The Third-Party Doctrine has been criticized because, in the modern era, one must share private information to take part in modern activities, which makes this information not actually given voluntarily.[150]

Simply because a person chooses to give a store personal information to receive a coupon does not mean that the consumer gave permission to data mining companies to analyze that data. The Third-Party Doctrine takes away consumers' interests in privacy by stating that voluntary distribution of PII relinquishes Fourth Amendment protection.[151] A consumer who voluntarily gives away PII should have the same rights as a consumer who does not give away any PII. Accordingly, the Third-Party doctrine should be improved to fully protect all consumers from unwanted third-party interaction.

CONCLUSION

Data collection is at the forefront of new regulations and policies. The FTC and Executive branch have proposed new ways to protect consumer privacy.[152] State laws from Massachusetts, California, Connecticut, and Virginia go to great lengths to protect consumer privacy. The laws protect PII and require disclosure and notice of third parties used

148. Thompson II, *supra* note 55.

149. *Id.*; *see also* i*nfra* notes 69 through 77 and accompanying text.

150. Thompson II, *supra* note 55.

151. *Id.*

152. *Protecting Consumer Data*, *supra* note 35 at v-viii; Obama, *supra* note 42 at 2.

by merchants.[153] Still, the current state of consumer protection severely lacks a true defense to company infringement on PII.

The proposed regulation included company based action for notice, choice and third-party collection. The regulation also prohibited selling consumer PII and suggests a client-based relationship with data mining companies and stores. This Article further suggests imposing a fine on merchants who do not follow the regulations. Further, the FTC must strengthen the enforcement of all consumer protection regulations. This article also suggests that the Third-Party Doctrine from *Katz v. United States* be overturned as it destroys consumers' right to privacy under the Fourth Amendment.[154]

Protection of consumer privacy is extremely important as it creates trust between the consumer and the merchant. In order to maintain this trust, consumers and businesses must work together to balance privacy and marketing. Without marketing, companies may not be able to increase revenue enough to sustain a place in the market. But, individual privacy should trump an increase in revenue and therefore merchants should not exploit consumers for their information for marketing purposes. Data mining companies and analysis can be a useful tool for businesses, so the practice must still remain with stronger regulations.

Target learned the hard way that direct marketing and data mining violate consumer privacy.[155] Many consumers enjoy saving money on purchases, but the price of giving away PII to a merchant or data mining company may not be worth the savings. Sending advertisements, coupons, emails, or flyers seems harmless but the way companies and third party data mining companies receive consumer information infringes on consumer privacy rights and requires stronger protection.

---

153. *See infra* notes 120 through 134 and accompanying text.
154. Thompson II, *supra* note 55.
155. Duhigg, *supra* note 1.