Keeping Your Personal Information Personal: Trouble for the Modern Consumer

Eugene E. Hutchinson

Follow this and additional works at: http://scholarlycommons.law.hofstra.edu/hlr

Part of the Law Commons

Recommended Citation
Available at: http://scholarlycommons.law.hofstra.edu/hlr/vol43/iss4/7

This document is brought to you for free and open access by Scholarly Commons at Hofstra Law. It has been accepted for inclusion in Hofstra Law Review by an authorized administrator of Scholarly Commons at Hofstra Law. For more information, please contact lawcls@hofstra.edu.
NOTE

KEEPING YOUR PERSONAL INFORMATION PERSONAL: TROUBLE FOR THE MODERN CONSUMER

I. INTRODUCTION

The online market is continuously growing and expanding, with many benefits to the consumer.\(^1\) Online purchasing and web browsing make consumers' lives much easier.\(^2\) But the ease of online activities comes with a cost.\(^3\) Companies are collecting, storing, and using consumers' personal information more expansively than ever before—and eroding privacy in the process.\(^4\) Often consumers share their

---


2. See THE WHITE HOUSE, CONSUMER PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 5-6 (2012), available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. For consumers specifically, there are a host of advantages for online shopping. For example, online shopping saves consumers time by being able to shop in their own homes; it is easier to find the lowest prices; the Internet never closes so you can shop at any time; and you can look for specific merchandise that includes model number, style, size, and color that you want to purchase, thus greatly increasing product availability. ships2door, Advantages to Online Shopping and Its Disadvantages, EBAY (Nov. 17, 2013), http://www.ebay.com/gds/Advantages-of-Online-Shopping-and-its-Disadvantages-/10000000177896151/g.html.


personal information with retailers or other companies by their choice ("approved companies"), but are unaware that the information is thereafter being given or sold to third parties. Approved companies pass information on to what are known as data brokers—companies that are in the business of collecting, storing, and selling consumer information. In many instances, these data brokers gather consumers’ information without their knowledge. They can also track everything a consumer does on the Internet: where she shops, what she buys, how she is feeling, and essentially anything she browses on the web.

Unfortunately for consumers, current laws do not adequately address this type of consumer privacy breach, and do not afford the protection consumers deserve with respect to data selling practices. Part II of this Note will give an overview of the data market, including the data collection and storage practices of approved companies and data brokers, and the current legislative landscape for the protection of consumer privacy online. Part III will describe in detail the harm that is caused by the unauthorized collection and dissemination of personal identification information, the ineffectiveness of the current legislation and regulation tactics to protect consumers from that harm, and consumers’ inability to bring successful actions to defend their privacy in court. Finally, Part IV proposes implementing legislation aiming to protect consumers’ personal identification information by use of opt-in consent, establishing a registry of data brokers, and creating a private right of action, so that consumers can successfully bring lawsuits when companies violate their privacy rights and hold those companies accountable.

II. A BRIEF HISTORY OF THE DATA MARKET, REGULATION, AND THE RIGHTS AT STAKE

While data collection has been occurring for many years, the capabilities for data collectors have expanded in the online age. This has led to an ever-expanding data market, which will be described
Subpart A will introduce and explain how companies collect consumers’ personal information, focusing on the online collection methods, and will discuss the vast data market as it exists today. With this data collection, however, come privacy concerns. Subpart B will give a background on the establishment of privacy rights in the United States, and the legislative and regulatory framework in place, which is aimed at protecting that right with regards to consumers’ personal information.

A. The Data Collection Process and the Market It Created

Computers and Internet technology have made it easier for companies to gather consumers’ personal information and track their habits online. Approved companies gather a variety of information from consumers, known as “personally identifiable information” (“PII”). The federal government defines PII as:

information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.

This information includes, but is not limited to, a customer’s name, address, telephone number, and email address. Other information can be gathered and stored through a consumer’s browsing habits, such as the types of products purchased and their prices.

---

14. See infra Part II.A.
15. See infra Part II.A.
16. See infra Part II.C.
17. Devin W. Ness, Note, Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn’t Spell the End for Privacy as We Know It, 31 CARDozo ARTS & ENT. L.J. 925, 932-33 (2013) (describing how recent advances in technology have driven the price of information collection, sharing, and storage down making it easier for companies to gather personal information).
18. See THE WHITE HOUSE, supra note 2, at 10 (defining PII as any data, including aggregations of data, which is linkable to a specific individual).
The data is collected through accessing a variety of online and offline consumer activities revealing personal information disclosed in connection with such activities. These activities include: purchasing products online; browsing the Internet; filling out a form or survey to get a coupon; social media; subscribing to websites; or entering sweepstakes. Consumer data is also collected through the purchase of mobile applications.

Approved companies, whether small retailers or Internet giants, such as Google, collect consumer information for a variety of purposes. The consumer is aware of some of this collection activity and benefits from it, such as when the consumer provides information to verify identity for purchases, to ship a purchase, or to further the company’s internal marketing purposes for generating focused advertisements. Companies defend such collection by asserting that it is for the good of consumers. For example, Google’s privacy policy provides a laundry list of the uses for consumer data that is beneficial to the consumer. This list includes making ads more effective; improving users’ experiences; protecting against fraud and other security risks; and improving Google products. Privacy primarily becomes an issue when the information is shared outside of the approved company. In many instances, approved companies share that personal information with a third party. This type of transaction has developed a vast market for...
data, in which users' personal information is being used to make a profit. Consumers' personal information is a hot commodity and has a value that is unknown to the average consumer when they disclose it to the approved companies.

When approved companies gather personal information and disseminate it to third parties, it is often to data brokers—companies that gather, analyze, store, and sell personal online information—which has, in turn, given rise to the data market. Data brokers exist largely unknown to the average consumer. Although they have no direct contact with consumers, data brokers collect, manipulate, and share consumers' information. Because they are generally unaware of these practices, consumers rarely have a choice about how the data brokers are obtaining and using their information and would struggle to get an explanation as to the dissemination of this information.

Data brokers generally collect their information from three different sources: (1) the government (both state and federal); (2) publicly available sources, including social media, blogs, and the Internet; and (3) commercial data sources, like approved companies. Today, the most common resource of collection is likely through commercial data sources, and collection is perhaps easiest online. In some instances, consumers provide information directly to approved companies "through loyalty card programs at grocery or retail stores, website registrations, dissemination of personal information to third-party app vendors, and claimed this was done without their consent. Other lawsuits concerning similar instances are discussed further below. See infra Part III.C.

32. See FED. TRADE COMM’N, supra note 20, at 23; Pasquale, supra note 30.
33. See, e.g., FED. TRADE COMM’N, supra note 20, at 23. According to a study conducted by the Federal Trade Commission, five data brokers (companies that collect and sell consumer data) collectively generated over $196 million of revenue in 2012. Id.
35. FED. TRADE COMM’N, supra note 20, at 46; Ramirez, supra note 21.
36. FED. TRADE COMM’N, supra note 20, at 3. For example, data brokers create what are known as “data elements” and “segments.” Id. at 19-21. These segments may be created by combining various sets of data compiled for an individual to create lists or categories of similar individuals and developing predictions of a consumer’s interest by looking at purchase history and consumers with similar data sets. Id.
37. Id. at 48-49; see also Pasquale, supra note 30 (describing inaccurate information held by data brokers which consumers are unable to correct).
38. FED. TRADE COMM’N, supra note 20 at 11-15. In a report studying nine different data brokers, approximately half of the data broker companies reported they collected their data from government sources, and six reported they collected from publically available sources. Id. at 7-9, 13-14. However, all but one reported they collected from commercial sources. Id. at 13-14.
warranty registrations, contests, surveys and questionnaires," and that data is then shared with data brokers. Data brokers (and approved companies) may also collect information about consumers' online locations and activities. This information may include a consumer's IP address, the browser used, and activities on various websites, such as purchase history and browsing habits. Data brokers sometimes enter into cooperative agreements with approved companies, who provide information about their customers (such as purchase information, postal addresses, e-mail addresses, and transaction history) in exchange for information that elaborates upon customer lists or identifies new customers. Customer lists and customer information have long been understood to be company assets, and the ease of online data collection has made those assets more valuable than they have ever been.

Joel Stein of the New York Times illustrated the chilling reality of the amount of data that is collected and stored ready to be accessed or viewed by these data brokers. Stein contacted a number of data brokers just to see how much information they had on him, and what they could do with that information. He gave only his name and email to Michael Fertik, the CEO of online data services company Reputation.com. Within only a few hours, Fertik called Stein back and read his social security number to him. It was virtually effortless for Fertik to obtain Stein's social security number with the use of seemingly harmless information: a name and email address.

41. Id.
42. Id.
45. Stein, supra note 8.
46. Id.
47. Id. Reputation.com claims to be "the world's leading provider of online reputation products and services." About-Us, REPUTATION, http://www.reputation.com/about-us (Sept. 2, 2015). The company assists individuals in understanding their online reputation and gives them "the tools to monitor, manage, and secure information on the Internet." Id.
48. Stein, supra note 8.
49. Id.
The information shared on the web is not just identification information; data brokers also collect and share intimate personal information, which users thought was confidential, such as health records.50 For example, a company called MEDbase 200, which sells lists of medical industry information, has lists of people who have been victims of rape and people who suffer from erectile dysfunction, alcoholism, and AIDS.51 These lists included 1000 names, and were sold at a price of seventy-nine dollars per list.52 Even sensitive medical information is available for purchase.

B. The Right to Privacy in the United States and the Current Landscape for Consumer Privacy Protection

While not expressly written in the Constitution, the Supreme Court has recognized a right to privacy embedded within the First, Third, Fourth, Fifth, and Ninth Amendments.53 The right of privacy is now long-recognized by Americans and concerns them greatly.54 Long before the age of the online consumer, Samuel Warren and Louis Brandeis


51. Kashmir Hill, Data Broker Was Selling Lists of Rape Victims, Alcoholics, and ‘Erectile Dysfunction Sufferers,’ FORBES (Dec. 19, 2013, 3:40 PM), http://www.forbes.com/sites/kashmirhil/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers. The testimony of Pam Dixon, the executive director of the World Privacy Forum, revealed the existence of these lists. Id. MEDbase 200 is an Illinois company owned by a direct mail advertising company called Integrated Business Services Inc. Id. That company’s president claimed that the company never maintained an actual list of rape victims, and that it was a list of health conditions and ailments that was used for a hypothetical file for an internal test. Id.

52. Id.

53. See Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965). In Griswold, the U.S. Supreme Court held that the First Amendment has a “penumbra” where privacy is protected from the federal government, and for the first time recognized a right to privacy embedded within the Constitution. Id. But see James P. Nehf, Recognizing the Societal Value in Information Privacy, 78 WASH. L. REV. 1, 34 (2003) (noting that the Supreme Court has “not found much protection within the ... Constitution against information collection and disclosure” for information other than health and sex information). James P. Nehf argues that the Court’s decisions have “only marginal relevance to the problem of databases” because “[t]he Supreme Court has assumed that privacy is about protecting highly personal information,” and that “we have no constitutionally protected expectation of privacy when we permit our information to be accessed by a third party.” Nehf, supra, at 33. Constitutional law doctrine is not likely to provide effective privacy protection for most database problems. Id. at 35.

54. Id. at 8-16. For example, the Supreme Court has held that Americans have a right to make decisions about their bodies and private lives without interference from the government. See Roe v. Wade, 410 U.S. 113, 152-53 (1973). In Roe, the Court found there to be a Constitutional guarantee to privacy, as a personal right deemed fundamental or implicit. Id. The Court held that a woman’s decision on whether or not to terminate her pregnancy was a protected right and that a Texas law banning abortion was unconstitutional. Id.
brought attention to the right of privacy in an 1890 article published in the Harvard Law Review. Warren and Brandeis advocated for the protection of the person and securing in the individual the right “to be let alone,” which laid the foundation for many of the torts grounded in privacy law. Warren and Brandeis wrote of the invasion of “the sacred precincts of private and domestic life” caused by “instantaneous photographs and newspapers.” The scholars accurately predicted the dangers modern technology would pose to one’s right to privacy.

Privacy has further been described by some scholars as “control over when and by whom the various parts of us can be [seen] by others.” This type of privacy relates directly to consumers sharing their personal information online. Consumers want privacy over their information online, and the ability to control the collection, use, and distribution of it. The government has acknowledged the privacy right of control over personal information and enacted measures at the federal level to protect that right in certain industries where personal information is collected. The legislative framework applicable to personal information, as it currently stands, is comprised of laws that only apply in certain situations to certain sectors and industries.

The following types of entities and industries have at least some sort of privacy of personal information governance: government agencies, motor vehicle departments, cable television operators,

56. Id. at 195; see also Dorothy J. Glancy, The Invention of the Right to Privacy, 21 ARIZ. L. REV. 1, 1-8 (1979) (describing Warren & Brandeis as the “inventors” of the right to privacy concept and providing historical and legal background to The Right to Privacy).
57. Id.
58. See Whalen v. Roe, 429 U.S. 589, 605 (1977) (acknowledging a “threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks”);
Warren & Brandeis, supra note 55, at 195. Warren and Brandeis warned that “mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’” Warren & Brandeis, supra note 55, at 195.
60. Avner & Abril, supra note 59, at 1009.
61. Id.
62. PAULA SELIS ET AL., CONSUMER PRIVACY AND DATA PROTECTION: PROTECTING PERSONAL INFORMATION THROUGH COMMERCIAL BEST PRACTICES 14-21,
companies renting or selling video tapes;\textsuperscript{67} banking and finance;\textsuperscript{68} and electronic communications.\textsuperscript{69}

The Privacy Act of 1974 ("Act"),\textsuperscript{70} perhaps best illustrates the government's concern over the protection of PII. The Act governed the "collection, maintenance, use, and dissemination" of PII of individuals that federal agencies maintain in systems of records.\textsuperscript{71} The purpose of the Act was to provide "safeguards for an individual against an invasion of personal privacy" by requiring agencies to do the following: permit an individual to control the information collected; gain access to that information; collect the information for a lawful purpose and ensure the information is current and accurate for that purpose; and subject themselves to civil suit for violation of the Act.\textsuperscript{72}

The basis for the Act was a code of fair information practices that have come to be known as the Fair Information Practice Principles ("FIPP").\textsuperscript{73} A U.S. government advisory committee first proposed the FIPP "in response to concerns about the consequences computerized data systems could have on the privacy of personal information."\textsuperscript{74} The widely adopted principles of the FIPP are listed as follows: "[c]ollection limitation;\textsuperscript{75} "[d]ata quality;\textsuperscript{76} "[p]urpose specification;\textsuperscript{77} "[u]se
HOFSTRA LA W REVIEW

limitation;”78 “[s]ecurity safeguards;”79 “[o]penness;”80 “[i]ndividual participation;”81 and “[a]ccountability.”82 In addition to establishing the FIPP, the Act prohibited the disclosure of an individual’s PII absent the written consent of the individual and provided a means by which an individual could access and amend the records as needed.83

While the Act was solely concerned with privacy protection of personal information collected by government agencies, Congress has expressed its desire to extend such protection to information collection by private entities, both online and off, by enacting laws such as the Gramm-Leach-Bliley Act (“Gramm Act”).84 The Gramm Act requires financial institutions to provide each consumer with a privacy notice explaining what information they collect from the consumer, where that information will be shared, how that information will be used once shared, and how that information will be protected from further dissemination.85 Further, the privacy notice must disclose consumers’ right to opt out of the information being shared with unaffiliated parties.86 While Congress has clearly shown a desire to protect PII on a broad scale,87 it has not moved to implement laws that specifically address the more recent problem of online sharing of consumer data between approved companies and data brokers.88

78. Id. ("Personal Information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.").
79. Id. ("Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.").
80. Id. ("The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.").
81. Id. ("Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge a denial of those rights.").
82. Id. ("Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.").
86. Id.
87. U.S. GOV'T ACCOUNTABILITY OFFICE, supra note 40, at 7-12 (demonstrating that the Gramm Act is just one of the measures Congress uses to protect consumers’ personal identification information). For example, Congress passed the Fair Credit Reporting Act ("FCRA") in 1970, to protect the security and confidentiality of personal information collected or used to help make decisions about individuals’ eligibility for credit products, insurance, or employment. 15 U.S.C. § 1681(a) (2012); U.S. GOV'T ACCOUNTABILITY OFFICE, supra note 40, at 8.
88. U.S. GOV'T ACCOUNTABILITY OFFICE, supra note 40, at 7 ("Currently, no comprehensive federal privacy law governs the collection, use, and sale of personal information by private-sector companies."). Note that Congress has enacted a law to protect personal information online, but only that information which is disclosed by children. Children’s Online Privacy Protection Act, 16 U.S.C. § 6502 (2012) (establishing guidelines for websites which collect personal information from
While certain companies' online collection of personal information falls outside the scope of any enacted federal laws, there have been some legislative efforts at the federal level to protect the privacy of consumers' personal information online. One such measure was a 2011 Congressional bill, introduced by Senators John Kerry and John McCain, known as the Commercial Privacy Bill of Rights Act of 2011 (“2011 CPBRA”). The 2011 CPBRA aimed to provide protection for the "collection, use, and transfer of consumer data" online by placing "substantive requirements on covered entities reflecting each of the [FIPPs]." Moreover, the 2011 CPBRA attempted to apply the FIPPs to both for-profit and non-profit online companies in an effort to establish "comprehensive, baseline protections for consumer data." Unfortunately for consumers, the 2011 CPBRA was never enacted and died in Congress.

Senior Senator Robert Menendez, from New Jersey, introduced a similar piece of legislation under the same name to Congress in 2014, but that Bill was short-lived, as well.


S. 799, 112th Cong. (1st Sess. 2011); CDT Top-Level Analysis, supra note 89, at 1. Speaking to the necessity of the 2011 CPBRA, John Kerry stated: "If there was no law to stop [a] person from collecting or selling that personal information collected, you'd feel beyond violated." Jacqui Cheng, Consumer Groups Skeptical About Kerry-McCain Privacy Bill, ARSTECHNICA (Apr. 12, 2011, 4:27 PM), http://arstechnica.com/tech-policy/2011/04/consumer-groups-skeptical-about-new-kerry-mccain-privacy-bill (internal quotations omitted). He further went on to say: "It goes on unregulated every day in the digital world .... Right now, there is no law protecting the information that we share." Id. (internal quotations omitted).

CDT Top-Level Analysis, supra note 89, at 1; Cheng, supra note 90.

CDT Top-Level Analysis, supra note 89, at 1.


Even President Obama has expressed his concern over the protection of personal information by recommending his own Consumer Privacy Bill of Rights in 2012 ("2012 CPBR"). The President’s 2012 CPBR is described as a framework of protections that are “necessary to preserve consumer trust.” The goal of this proposal was to apply the “comprehensive, globally recognized . . . FIPPs" to the interactive and highly interconnected environment in which we live and work today.

Furthermore, the Federal Trade Commission ("FTC") has developed initiatives supporting self-regulation in the online industry that provides consumers with transparency regarding the data collection industry and promotes use of “Do Not Track” mechanisms and opt-out options from data collection. Do Not Track mechanisms allow consumers to choose to stop the tracking of their information by a particular approved company or data broker. Opt-out clauses simply provide consumers the option to choose not to have a company obtain and use their personal information. Generally, the FTC will take enforcement action to ensure companies live up to the promises made to the consumers to safeguard their information. The FTC receives its authority to enforce these actions from the Federal Trade Commission Act ("FTC Act"). While it contains no express grant of authority to protect privacy, other government entities accept that the FTC Act authorizes the FTC to levy penalties on approved companies found violating their own written policies and deceiving consumers.

96. THE WHITE HOUSE, supra note 2, at 1.
97. Id.
98. See FED. TRADE COMM’N, supra note 4, at 7-14.
99. THE WHITE HOUSE, supra note 2, at 12-13; see also Why We Need a “Do-Not-Track” Mechanism to Protect Consumers’ Online Privacy, CONSUMER FEDERATION OF AM., http://www.consumerfed.org/pdfs/Why-We-Need-a-Do-Not-Track-Mechanism.pdf (last visited Sept. 2, 2015) (explaining how a Do Not Track mechanism would effectively limit the collection of consumers’ personal information without their consent).
100. See FED. TRADE COMM’N, supra note 4, at 4 (discussing the research of innovations to make opting out easier).
101. Enforcing Privacy Promises: Making Sure Companies Keep Their Privacy Promises to Consumers, FED. TRADE COMMISSION, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Sept. 2, 2015). The FTC has brought "[thirty-two] legal actions against organizations that have violated consumers’ privacy rights, or misled them by failing to maintain security for sensitive consumer information." Id.
103. U.S. GOV’T ACCOUNTABILITY OFFICE, supra note 40, at 11 ("For example, if [an online retailer] had a written privacy policy stating it would not share . . . information with . . . third parties.
III. AN UNREGULATED DATA MARKET INVADES CONSUMER PRIVACY WITHOUT REDRESSABILITY

The data collection process has created a vast open market of PII, which continues to grow. The rate of accumulation and dissemination of PII is increasing, and there are currently no federal regulations or laws in place to ensure the proper use and collection of this data. Thus, the data industry remains free to collect, store, and disseminate consumers' personal information without restriction, which erodes consumers' privacy rights when browsing the web and conducting online transactions, and leaves consumers with limited ability to enforce and protect these rights.

Below, Subpart A will give an overview of the financial and the personal harm that data collection causes. Subpart B will discuss the federal government's inability to effectively control data collection practices under the current legislative regime. Lastly, Subpart C will discuss the difficulties consumers face in protecting themselves from companies' unauthorized data collection and dissemination to third parties, enforcing their privacy rights, and seeking redressability through the courts.

A. Unauthorized Data Collection Causes Financial and Personal Harm to the Consumer

Unauthorized collection and sharing of personal data causes both economic and personal harm to consumers. First, this Subpart will describe the financial harm to consumers caused by data breaches arising from the storage of accumulated personal information. Next, this


105. See COMM. ON COMMERCE, SCI. & TRANSP., supra note 4, at 29-32; U.S. GOV'T ACCOUNTABILITY OFFICE, supra note 40, at 7; Morris & Lavandera, supra note 104.

106. See infra Part III.A–C.

107. See infra Part III.A.

108. See infra Part III.B.

109. See infra Part III.C.


111. See infra Part III.A.1.
Subpart will describe the more personal harm at risk—the erosion of privacy and trust in online transactions.\textsuperscript{112}

1. Financial Harm

Identity theft harms consumers financially, costing consumers millions of dollars each year.\textsuperscript{113} Many identity thefts are the product of breaches in approved companies' or data brokers' databases of personal information collected from consumers.\textsuperscript{114} Consumers may take precaution when divulging their information to avoid the effects of a breach, but they are unable to prevent collection and storage of their personal information if they are unaware it is occurring.\textsuperscript{115}

Those who collect data do not usually gather personal information merely for a one-time use and then discard it; companies and data brokers keep this information indefinitely, leaving it vulnerable to invasion by hackers.\textsuperscript{116} In one recent twelve-month stretch, hackers exposed the personal information of 110 million Americans and gained unauthorized access to 432 million accounts.\textsuperscript{117} Measured since 2005, the Identity Theft Resource Center has reported 5377 breaches, as of June 9, 2015,\textsuperscript{118} which accounted for the disclosure of 786,098,214

\textsuperscript{112} See infra Part III.A.2.


\textsuperscript{114} See William Roberds & Stacey L. Schreft, Data Breaches and Identity Theft, 56 J. MONETARY ECON. 918, 919-20 (2009) (defining data breach as occurring when "an unauthorized party is able to access personal data that has been collected by an organization" and describing the relationship between data breaches and identity theft).

\textsuperscript{115} See Fed. Trade Comm'n, supra note 4, at 8; Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1883-93 (2013) (explaining the problems with consumer consent when consumers are seemingly fully informed and rational and describing privacy self-management of consumers and its pitfalls). As described above, consumers share their personal information with approved companies who may disseminate that information to data brokers. See supra notes 34-44 and accompanying text.

\textsuperscript{116} See Fed. Trade Comm'n, supra note 20, at 17. Some data brokers store all data indefinitely, even if that information is later amended. Id. at 16-18. For example, they explain that even if a consumer's information is outdated, it is important to keep the consumer's address history in order to verify information accuracy. Id. at 18.

\textsuperscript{117} Pagliery, supra note 113.

In 2013, identity theft topped the list of types of consumer complaints to the FTC at 290,056. A February 2013 identity fraud report, composed by Javelin Strategy & Research, found that, in 2012, nearly $21 billion was stolen in connection with identity fraud. With PII becoming even more readily available from data brokers, as evidenced by the increasing storage of such information, a rise in these crimes is reasonably foreseeable. In some instances, data brokers have even sold consumers’ personal information directly to those committing the frauds. Without greater transparency and more effective regulation, personal data is not safe in the possession of data brokers.

2. Erosion of Privacy

Equally important to the physical harm caused by data collection is the personal harm caused by the erosion of one’s expected privacy, and the subsequent invasion of privacy when surfing the web or engaging in online transactions. The FTC has acknowledged that privacy harms might arise from unanticipated uses of data, such as “the unexpected revelation of previously private information, including both sensitive information (e.g., health information and precise geolocation information) and less sensitive information (e.g., purchase history and employment history) to unauthorized third parties.”

119. Data Breaches, supra note 118. The Center’s breach list is a “compilation of data breaches confirmed by various media sources and/or notification lists from state governmental agencies.” Id. The Center asserts “[b]reaches on this list typically have exposed information that could potentially lead to identity theft, including Social Security numbers, financial account information, medical information, and even email addresses and passwords.” Id. The Center defines “breach” as follows: “[A]n incident in which an individual name plus a Social Security number, driver’s license number, medical record or financial record . . . is potentially put at risk because of exposure.” Id.


122. See id. at 11.


124. See id.; see also FHCP Soc. Team, Data Brokers Sell Your Personal Information Online, FLA. HEALTH CARE PLANS (Oct. 30, 2014), http://www.fhcp.com/blog/data-brokers-sell-personal-online-information (educating consumers about the realities of data brokers’ activities).

125. See Shaun B. Spencer, Reasonable Expectations and the Erosion of Privacy, 39 SAN DIEGO L. REV. 843, 870-73 (2002) (discussing the erosion and exploitation of privacy on the Internet); see also FED. TRADE COMM’N, supra note 4, at 7-9 (discussing the broad consensus among commentators that consumers need basic privacy protections for their personal information).

126. FED. TRADE COMM’N, supra note 4, at 8.
Consumers are equally concerned with the loss of their privacy in their online activity.127 There are two major online privacy concerns for consumers: (1) the "vulnerability to the unauthorized gathering and misuse of personal information;" and (2) the lack of the "ability to control" the use of personal information they share.128 The feeling of vulnerability involves the potential risks that arise when personal information is revealed, which are described above.129 The ability to control is the extent to which consumers think they can prevent personal information from being disclosed online without their knowledge.130 Because of the convoluted language found in privacy agreements governing online data collection practices, users are sharing personal information without knowing if it will be shared with third parties or with whom the information is shared, increasing the consumers' concern that they lack the ability to control the use of their personal information.131 Moreover, the legislation and FTC enforcement policies have been unsuccessful in protecting consumers' expectation of privacy, and consumers have been unable to obtain judicial remedy through the courts.132

The concern over a lack of ability to control the collection and use of one's personal data is legitimate.133 Consumers may be harmed if data is collected inaccurately and they have no chance to correct the error.134

127. See Katy Bachman, Consumer Confidence in Online Privacy Hits 3-Year Low: Most Afraid of Businesses, Not Government, ADWEEK (Jan. 28, 2014, 10:04 AM), http://www.adweek.com/news/technology/consumer-confidence-online-privacy-hits-3-year-low-155255. According to one online survey, ninety-two percent of Internet users worried about their privacy online in 2014. Id. The concerns chiefly came from businesses sharing their personal information with other companies. Id.


129. See Bandyopadhyay, supra note 128, at 32-33; infra Part III.A.1.

130. Id.

131. See infra Part III.B.

132. See supra Part II.B; infra Part III.B; see also Adam Cohen, Will We Ever Get Strong Internet Privacy Rules?, TIME (Mar. 5, 2012), http://ideas.time.com/2012/03/05/will-we-ever-get-strong-internet-privacy-rules (discussing the failure of government to protect the privacy of consumer information).

133. See FED. TRADE COMM'N, supra note 20, at 48.

134. See Ian Kerr & Jessica Earle, Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy, 66 STAN. L. REV. ONLINE 65, 68-71 (2013); see also FED. TRADE COMM'N, supra note 20, at 48 (describing risks of use of data brokers for risk mitigation when personal data is not accurate).
For example, one of the services data brokers offer is risk mitigation.\textsuperscript{135} Approved companies use data brokers to verify a customer's information before making a transaction.\textsuperscript{136} However, a customer may be wrongfully denied from engaging in a transaction based on an error in the data broker's risk mitigation information.\textsuperscript{137} When the consumer is unaware the data broker has this particular information, or even who the broker is, they are often unable to prevent this problem from recurring.\textsuperscript{138} This repeating error may adversely affect not only a consumer's ability to shop online, but also a consumer's credit report.\textsuperscript{139}

\textbf{B. The Current Legislative and Regulatory Landscape Fails to Protect Consumers and Uphold an Expectation of Privacy}

As discussed above, there is no legislation currently in place to protect consumers in transactions with approved companies, and recommendations by the FTC have the wrong focus, rendering their proposals ineffective.\textsuperscript{140} In its report on data brokers, the FTC recommended that Congress consider legislation that requires data brokers to give consumers "the ability to opt-out of having it shared for marketing purposes."\textsuperscript{141} Opt-out agreements certainly give consumers some control over their personal information, but they fall short of offering optimal control.\textsuperscript{142} This is true because companies do not in actuality want consumers to opt-out, and thus, will try to prevent them from doing so.\textsuperscript{143} Companies have no incentive to make their privacy policies any clearer or more transparent, as they benefit from consumers' confusion and apparent consent to the misunderstood and uninhibited use of their personal information.\textsuperscript{144} If the user opts-out, the company will not be able to collect that user's valuable personal information.\textsuperscript{145} Therefore, these opt-out agreements are often very long and confusing, and they have been described as something that you need "the eyes of an

\textsuperscript{135} Fed. Trade Comm'n, supra note 20, at 32-33.  
\textsuperscript{136} \textit{id.}  
\textsuperscript{137} \textit{id.} at 48.  
\textsuperscript{138} \textit{id.}  
\textsuperscript{139} \textit{id.}  
\textsuperscript{140} See supra Part II.B.  
\textsuperscript{141} Fed. Trade Comm'n, supra note 20, at viii.  
\textsuperscript{142} Mike Hatch, The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century, 27 WM. MITCHELL L. REV. 1457, 1494-95 (2001) (explaining that "under an opt-out system, information may be shared and made public unless a person instructs the entity to keep it confidential" and that under such a system, a consumer must say "stop" to prevent information from being collected).  
\textsuperscript{143} \textit{id.} at 1496-97.  
\textsuperscript{144} \textit{id.}  
\textsuperscript{145} See supra note 33 and accompanying text.
eagle” and “a law degree” to locate and fully understand. As a result, consumers frequently either choose not to read them or simply do not understand them. Thus, many consumers do not appreciate or exercise the “right” to opt-out. This fact leaves opt-out agreements largely ineffective in protecting consumer privacy, but rather effective in giving data companies what they want—consumers’ personal data.

Confusing privacy policies also give consumers a false sense of security about the safety of their information. Often, approved companies post privacy policies voluntarily, which creates an appearance to consumers that they can trust the website with their personal information and that it will not be shared without their consent. In one poll of Internet users, seventy-five percent of users believed that “[w]hen a website has a privacy policy, it means the site will not share [their] information with other websites and companies.” But, in truth, these companies are creating illusory promises, and the consumers’ data may be shared unknowingly.

An example of such a confusing privacy agreement is Google’s user agreement. Google states in its user agreement that it provides clear information to its consumers with regard to the use of their personal information; but upon review of the agreement, such use is not so clear. First, the policy uses inconsistent terms when describing

146. Hatch, supra note 142, at 1497.
147. Id.
148. Id. at 1496-98. In his 2001 article, Mike Hatch describes three specific problems with opt-out mechanisms; a successful opt-out system is conditioned upon: (1) “individuals being able to understand how companies are using their personal information;” (2) “individuals getting meaningful notice that they have the right to opt-out of this information sharing;” and (3) “consumers being able to effectuate their preference without undue convenience.” Id. at 1495.
149. See Shankar Vedantam, To Read All Those Web Privacy Policies, Just Take A Month Off Work, NPR (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 (explaining how consumers do not have the time to read lengthy privacy policies and, therefore, typically do not do so).
150. See Nehf, supra note 53, at 63.
151. Id.
152. JOSEPH TUROW ET AL., OPEN TO EXPLOITATION: AMERICA’S SHOPPERS ONLINE AND OFFLINE 3 (2005) (internal quotation marks omitted).
153. Id. at 17-18.
154. See Privacy Policy, supra note 25.
155. Id. In fact, a federal judge rejected a motion to dismiss by Google in “a privacy lawsuit claiming it commingled user data across different products and disclosed that data to advertisers without permission.” Jonathan Stempel, Google Must Face U.S. Privacy Lawsuit Over Commingled User Data, REUTERS (July 22, 2014, 1:52 PM), http://www.reuters.com/article/2014/07/22/us-google-privacy-lawsuit-idUSKBN0FR1XA20140722. When Google consolidated its privacy policy for different Google products into a single policy, consumers were upset because they never consented to the change and received no way to opt out. Id.
what information is collected such as “personal information,” “personally identifiable information,” “sensitive personal information,” and “content.” The vague word “content” is probably the most confusing and troublesome to those who actually take the time to read the lengthy policy. Content is an extremely broad term—especially considering all of the products Google offers that require users to input information. In addition to the self-titled search engine, Google controls YouTube, which the company can track and monitor video preferences, and operates Google Wallet, which contains credit card information and tracks the goods and products consumers purchase. These are just a few of the different services Google offers.

The term “content” is not defined in Google’s privacy policy or the company’s terms of service. The privacy policy states that Google will “not share personal information with [outside] companies” unless they receive a user’s consent. However, the terms of service state that Google services allow users to “upload, submit, store, send or receive content,” and gives Google, “a worldwide license to use, host, store . . . communicate, publish, publicly perform, publicly display and distribute such content.” The terms of service do not clarify that the “use” mentioned is in accordance with the privacy policy; that section contains no reference to the privacy policy. Thus, without a definition

156. Privacy Policy, supra note 25.
158. Id. A journalist from the Wall Street Journal was astonished after looking at his Google portfolio. Amir Efrati, Google’s Data-Trove Dance: Internal Debates Arise Over Using Collected Information and Protecting Privacy, WALL ST. J., http://www.wsj.com/articles/SB10001424127887324170004578635812623154242 (last updated July 30, 2013, 10:04 PM). Google had stored or tracked 134,966 emails, 6147 chats, 2702 contacts, 9220 YouTube videos watched, 117 apps downloaded on Google Play, 35 different passwords, 855 documents, 3 credit cards, information from 3 synched phones, and 64,109 searches. What Google Knows, WALL ST. J., http://www.wsj.com/news/interactive/GOOGLE0731 (last visited Sept. 2, 2015). Also, Google asserts that the journalist performs most of his searches around 8 AM Eastern Standard Time. Id. Maybe more concerning, Google listed his base location as Willunga, South Australia, which is inaccurate, since it was gathered from an old phone he gave to his mother in Australia. Id.
161. Privacy Policy, supra note 25.
163. Google Terms of Service, supra note 160. The terms of service simply say: “You can find out more information about how Google uses and stores content in our privacy policy . . . .” Id. This does not imply the terms will necessarily abide by the privacy policy, or that the policy provides the exhaustive list of “uses.” Id.
of "content," by accepting the terms of service, users may be consenting for Google to give away their personal information.\textsuperscript{164} This is likely very confusing to most users and potentially leads them to disclose their information unknowingly to outside companies, which may even further disseminate their personal information.\textsuperscript{165}

Even without the apparent discrepancy in the definition of the term "content," the privacy policy's description of what personal information is shared, and with whom it is shared, is confusing.\textsuperscript{166} The privacy policy asserts that Google will not share personal information without user consent, but then goes on to say that "sensitive" information will only be shared with "opt-in" consent.\textsuperscript{167} This mixing of terminology makes unclear what the difference is between "personal" information and "sensitive" information, what requires a user's consent, and to what the user has specifically consented to be shared by accepting the terms of service agreement.\textsuperscript{168} Moreover, the terms of service agreement does not offer any reference to somewhere a user could provide consent or opt-out of consent.\textsuperscript{169} Additionally, Google's privacy policy states that the company can share all information with all its affiliates, products, and "trusted businesses or persons."\textsuperscript{170} While the privacy policy claims to apply to all affiliates and services, it conversely declares its exclusion from services that have different privacy policies.\textsuperscript{171} This contradiction leaves questions about which services or products have different privacy policies, and what makes those policies different.

The FTC has shown that Google does not always adhere to its privacy policies as they are written.\textsuperscript{172} Google, perhaps more than other

\textsuperscript{164.} See id.

\textsuperscript{165.} See id. Google is constantly expanding its collection and analysis of data, helping to create a $50 billion per year advertising business. Efrati, supra note 158. Google typically does not reveal much about its internal data-handling practices, "fearing that discussing privacy related topics might hurt the company with consumers." Id.

\textsuperscript{166.} See Privacy Policy, supra note 25.

\textsuperscript{167.} Id.

\textsuperscript{168.} See id.

\textsuperscript{169.} Google Terms of Service, supra note 160.

\textsuperscript{170.} Privacy Policy, supra note 25. Google received much criticism over the privacy policy the company released in 2012, under which personal information would automatically be distributed across all Google platforms and which did not provide for users' opt-in or opt-out consent for that procedure. See, e.g., News Release, Nat'l Ass'n of Attorneys Gen., Attorneys General Express Concerns Over Google's Privacy Policy, available at http://www.naag.org/naag/media/naag-news (in the website's search bar enter "Google's Privacy Policy").

\textsuperscript{171.} Privacy Policy, supra note 25.

companies, because of its size, is under very strict scrutiny for its privacy policy and practices. Nevertheless, the company’s privacy policy remains confusing to the average consumer, causing government officials and privacy advocates to express their concerns. Following the release of Google’s new privacy terms in 2012, members of Congress sent a letter to Google asking it to describe how much control its users have over the sharing of their search history and whether there is a way to easily opt-out of this sharing. In a response letter, Google stressed that its approach to privacy had not changed. Google’s letter further stated that users of its products continued to have choice and control and that the new policy did not affect previous privacy settings. In its response, Google also claimed that private information remained private, that it was not collecting new data or selling users’ data, and that it will continue to use data liberation tools.

Despite these assurances, since the date of that letter, the FTC has found Google in violation of its own privacy policy, and consumers continue to challenge Google in court over privacy issues, despite the grim chance of redress.

As an Internet giant, Google is often in the spotlight for its privacy terms.

would not place tracking ‘cookies’ or serve targeted ads to those users,” which violated an earlier privacy settlement between Google and the FTC. Id. (revealing that Google settled for a record $22.5 million civil penalty).


177. Id.

178. Id. Data liberation tools were created by Google to allow users to access information created or imported into numerous Google products. Download Your Data: FAQ, GOOGLE, https://support.google.com/accounts/answer/3024190?hl=en (last visited Sept. 2, 2015).


181. See, e.g., Paula Rooney, Google, Web Security and Privacy in Spotlight at CeBit 2012,
share data that are not so easily identifiable.\textsuperscript{182} It is virtually impossible for the FTC to monitor every website to ensure that the data collection practices are consistent with their intended purpose.\textsuperscript{183} The FTC’s actions are generally grounded in the notion that approved companies and data brokers will self-regulate pursuant to the FTC’s guidelines; however, approved companies and data brokers have failed to do so.\textsuperscript{184} Additionally, the FTC only has the ability to enforce existing privacy and security settlements made with approved companies with regards to their privacy policies; it lacks the authority to issue sanctions when an approved company breaks the law.\textsuperscript{185}

FTC enforcement is also very complicated because of the vast number of companies collecting data.\textsuperscript{186} Since so many different data brokers of varying size exist, many are hard to identify.\textsuperscript{187} Usually only the largest brokers, or those that violate their policies most egregiously, are held accountable because they attract the public’s attention.\textsuperscript{188} Generally, though, there is very limited information known about the data broker industry, so many go unchecked.\textsuperscript{189} For example, the U.S. Census Bureau “does not assign a business classification code specific to information resellers,” and the FTC and Department of Commerce admit that there is no comprehensive list or registry of companies that engage

\textsuperscript{182} See Craig Timberg, \textit{Brokers Use ‘Billions’ of Data Points to Profile Americans}, WASH. POST (May 27, 2014), http://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362f5443d19_story.html.\textsuperscript{183} Marc Loewenthal, \textit{Internet of Things: Current Privacy Policies Don’t Work}, INFORMATIONWEEK (June 30, 2014, 9:06 AM), http://www.informationweek.com/big-data/hardware-architectures/internet-of-things-current-privacy-policies-dont-work/a/d-id/1278925.\textsuperscript{184} See Timberg, \textit{supra} note 182.\textsuperscript{185} See U.S. GOV’T ACCOUNTABILITY OFFICE, \textit{supra} note 40, at 4.\textsuperscript{186} See id. at 4-5. For example, the FTC has taken action against Internet giants such as Google for their data collection practices. See, e.g., Press Release, Fed. Trade Comm’n, \textit{supra} note 172. The FTC has taken action against data brokers who participated in particularly egregious activities, such as against data broker LeapLab, which was selling sensitive personal information, including social security and bank account numbers, to scammers who allegedly debited millions from the customers’ accounts. Press Release, Fed. Trade Comm’n, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers’ Accounts, Dec. 23, 2014, \textit{available at} https://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars. Many data brokers, however, exist largely unknown. See \textit{supra} note 35 and accompanying text.\textsuperscript{187} U.S. GOV’T ACCOUNTABILITY OFFICE, \textit{supra} note 40, at 4-5. While there are several privacy-related organizations and websites that maintain lists of information resellers, none of these lists claim to be comprehensive. Id. at 4.
in data broker practices. Compounding the issue, current statutes that contain a private right of action do not apply to most online consumer transactions, so many unauthorized collection practices go unpunished. Moreover, one specific problem with the data brokers existing behind the scenes is that consumers do not have access to the information the data brokers have collected and stored. The information held and shared could be inaccurate, but there is no law that requires data collectors to allow consumers to view the information they hold. Privacy advocates and members of Congress have argued that consumers should possess the right to view exactly what information data brokers have stored. If consumers had access to the data which had been shared, they could take precautionary steps to prevent fraud, avoid improper identity verification, and prevent other harms and inconveniences caused by data inaccuracies. One problem with granting consumers the right to check any data which is stored or collected is that there are so many sources collecting in so many different instances, that consumers would be unable to verify all the data available. Therefore, measures should be taken to control inaccuracies when the data is initially entered, not just once it is shared amongst data brokers.

C. Consumers’ Troubles in Successfully Bringing Civil Actions

Consumers have been allowed to bring class actions against approved companies for the unauthorized collection and use of personal information, but the litigation rarely survives a motion to dismiss. Courts routinely dismiss these actions for lack of standing and a failure to show sufficient causes of action to maintain a suit. Since consumers

190. Id. at 4-5.
193. Id. at 37. Congress has considered legislation that would allow consumers correct information stored with data brokers—most recently with a bill introduced into the Senate known as the Data Broker Accountability and Transparency Act, which aims to prohibit a data broker from obtaining or causing to disclose personal information. S. 2025, 113th Cong. (2014).
194. U.S. GOV’T ACCOUNTABILITY OFFICE, supra note 40, at 37.
195. Id.
196. Id.
198. See Joel R. Reidenburg, Privacy Wrongs in Search of Remedies, 54 HASTINGS L.J. 877,
are rarely successful in these class actions, companies are not being held accountable for their actions and have no incentive to stop invading consumers' privacy. These shortcomings will be illustrated by examples below.

Consumers have sought relief in class action lawsuits against Internet giants, such as Google, Apple, and Facebook. The courts, however, have been unable to provide adequate relief under the current legal structure and practice. Consumer plaintiffs rarely have a chance to even argue the merits of their case, as most of their claims are dismissed at the pleading stage for a lack of standing because they cannot establish injury. In In re iPhone Application Litigation, for example, consumers brought suit against Apple and a collection of mobile industry defendants for allegedly committing privacy violations by “illegally collecting, using, and distributing iPhone, iPad, and Apple App Store users’ personal information.” The court, while acknowledging that it “[did] not take lightly Plaintiffs’ allegations of privacy violations,” found the allegations were “clearly insufficient” to show standing under Article III of the Constitution. The requirements for Article III standing are: (1) an injury in fact; (2) that is fairly traceable to the challenged conduct; and (3) which has some likelihood of redressability. Courts repeatedly find that consumer plaintiffs in these actions cannot show an injury in fact—that they actually suffered an economic harm from the alleged unauthorized taking of

199. Id.
200. See infra notes 201-27 and accompanying text.
205. Id. at *1.
206. Id. at *4.
207. Id. at *3 (quoting Friends of the Earth, Inc. v. Laidlaw Env't Sys. (TOC), Inc, 528 U.S. 167, 180-81 (2000)).
consumer information. As a result, consumer claims are dismissed for lack of standing.

In a few instances, consumers were able to plead sufficient standing in privacy of information cases when bringing actions under federal statutes that create a private right of action, such as the Stored Communications Act ("SCA"). In Svenson v. Google Inc., the court found the plaintiff had standing for an SCA claim because, regardless of whether the plaintiff suffered any concrete, particularized injury, a plaintiff can demonstrate injury sufficient for Article III standing when bringing a claim under a statute that provides for a private right of action. However, while the Svenson court found standing under the SCA, it held that distribution of personal information to third parties, even if seemingly unlawful, was not in violation of the statute—which poses another legal obstacle consumer plaintiffs face when attempting to bring these actions.

In Svenson, consumers filed a class action against Google for sharing their personal information with third parties. The complaint alleged that when a consumer purchased applications in the Google Play store using Google Wallet, the company, after processing the payment, not only "automatically remit[ted] funds to the third-party vendor [but also provided] the [consumer's] name, email address, Google account name, home city and state, zip code, and . . . telephone number." Further, the user complained that, when purchasing the application, she was prompted to verify the purchase and then Google would process the

---

208. See, e.g., Google Android Consumer Privacy Litig., 2013 WL 1283236, at *6-7 (dismissing complaint in part for lack of standing and finding the plaintiffs did not plead facts sufficient to show injury); Yunker v. Pandora Media, Inc., No. 11-cv-03113, 2013 WL 1282980, at *3-5 (N.D. Cal. Mar. 26, 2013); In re iPhone Application Litig., No. 11-MD-02250, 2011 WL 4403963, at *4-7 (N.D. Cal. Sept. 20, 2011).


210. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012). Enacted in § 2702 of the United States Code, the SCA provides a private right of action when someone's information is improperly shared, in the following provision:

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service.

Id. § 2702(a)(1)-(2).


212. Id. at *2.

213. Id. at *7 ("Regardless of the merits of Plaintiff's policy arguments, this Court is without authority to alter the plain language of the statute . . . ").

214. Id. at *1-2.

215. Id. at *1.
payments, and remit the user’s information. However, the plaintiffs claimed that Google’s disclosure of the user’s name was not necessary to process the payment and that at no time did Google tell users that their information was being shared with the third-party vendors. Indeed, the information was made available to third-party application vendors as “shipping information,” even though no product was being shipped. Since no address was needed, and Google was supposed to conduct the credit card transaction, the disclosure was alleged to be both “unnecessary and unauthorized by the user.”

Although “[t]he SCA was enacted because the advent of the Internet presented a host of potential privacy breaches,” it does little to protect consumers from unauthorized and unnecessary data disclosures, because the statute has a narrow scope of information types that are protected. Courts have found that when a consumer gives personal information to a merchant, that transaction does not fall within that narrow scope of the SCA. Indeed, in Low v. LinkedIn Corp., the court held that “[t]he SCA is not a catch-all statute designed to protect the privacy of stored Internet communications” and acknowledged that there are problems that the SCA does not address. As an example, in Svenson, the court acknowledged the merits of a policy argument combating the unlawful disclosure of personal information to third parties, but held that it could not advance that policy through current legislation, including the SCA.

217. Id.
218. Id. at para. 52.
219. Svenson, 2014 WL 3962820, at *1. The Google Wallet privacy policy, as of the printing of this Article, still states that Google will share your personal information with a third party to “process your transaction and maintain your account.” Google Wallet Privacy Notice, GOOGLE, https://wallet.google.com/legaldocument?family=0.privacynotice (last modified June 30, 2015). This statement in the privacy policy is broader than the assertion in the Svenson action that the information was provided to the third-party vendor. See Complaint, supra note 216, at para. 52. If the sharing is unnecessary, Google still will provide a third party with your personal information—and, this third party may provide the personal information to data brokers, who consistently buy and sell personal information and disclose it to other third parties and are largely unknown by the consumer. See Google Wallet Privacy Notice, supra; Getting to Know You: Data, ECONOMIST, Sept. 13, 2014, at 5.
224. Low, 900 F. Supp. 2d at 1022 (internal quotation marks omitted).
225. Svenson, 2014 WL 3962820, at *7-8. The question for the Northern District of California court was whether contact information that the defendants sent to the third-party vendor was “contents of a communication” or “a record or other information.” Id. at *8. If it was contents of a
plaintiff's claims were dismissed. Moreover, the court found that the plaintiff could not maintain actions for breach of either contract or implied covenant of good faith.

IV. CONSUMER CONTROL, TRANSPARENCY & ACCOUNTABILITY: A LEGISLATIVE SOLUTION TO DATA MARKET DANGERS

While the FTC is diligently working to regulate the online data marketplace, the data market remains vastly unregulated, and legislation must be passed regarding data collection practices to ensure consumer protection. Advocacy groups are calling for legislation that would limit marketers' ability to collect or use data about individuals. As discussed below, legislation should include a private right of action, and a value should be given to consumers' personal information to allow them to prove injury and plead damages in court. If held accountable by way of consumers' civil actions, companies will be forced to care more about consumer privacy.

communication, the plaintiff would have adequately stated a claim. Id. at *7-8. The Ninth Circuit had previously held that individuals' names, addresses, telephone numbers, email addresses, dates of birth, and other identifying information were correctly characterized information as "contents of a communication '[when] the users had communicated with the website by entering their personal medical information into a form provided by a website.'" Id. at *8 (quoting In re Zynga PrivacyLitig., 750 F.3d 1098, 1107 (9th Cir. 2014)). The Zynga court distinguished this type of information from information that was automatically generated from a web browser, and characterized the former as "record information." See id. (clarifying the holding in Zynga). The Svenson Court, while acknowledging the distinction between the two types of information, did not read Zynga so narrowly to mean that only automatically generated data may constitute record information, and chose not mandate a conclusion that all information input by means of a form interface constitutes "contents of a communication" under the SCA. Id. at *9.

226. Id. at *9.
227. Id. at *3-5. As to the breach of contract action in Svenson, the court held that the plaintiff's identification of the "contract" was inadequate, and that the plaintiff referred to the wrong contract in her complaint. Id. at *4. More specifically, though, the court found that the plaintiff's allegations of breach of contract were conclusory and insufficient to plead her contract claim. Id. Other claims, such as a breach of state constitutional privacy, have also been dismissed by the California courts for similar reasons. Low, 900 F. Supp. 2d at 1025-26.


229. See Wendy Davis, Advocates, IAB Weigh in on Privacy Bill of Rights, CONSUMER WATCHDOG (Aug. 5, 2014), http://www.consumerwatchdog.org/story/advocates-iab-weigh-privacy-bill-rights. The advocates, including the American Civil Liberties Union, Center for Digital Democracy, Consumer Action, Consumer Confederation of America, Consumer Watchdog, Common Sense Media, and Privacy Rights Clearinghouse, sent a letter to the Commerce Department, which stated: "Industry self-regulation is not enough, and has failed to inform or protect consumers..." Id. (internal quotation marks omitted).

230. See infra Part IV.A.
231. See generally Eric C. Bosset et al., Private Actions Challenging Online Data Collection
opt-in clauses, not opt-out clauses, as they are the best way to ensure consumer privacy protection; new laws should force companies to utilize them for their data collection practices.\(^{232}\) Lastly, legislation should require data brokers to register with a national registry maintained by the government, so consumers can easily determine their existence and practices, and gain access to the information they may have collected.\(^{233}\)

**A. Legislation Protecting Personal Information Is Necessary and Should Include a Private Right of Action**

In order for consumers to maintain actions for unauthorized disclosure of personal information, legislation directly addressing consumer privacy is necessary and should include a private right of action. As discussed above, the current legislation in place to protect the privacy of Internet communications does little to protect consumers from unauthorized disclosure of their personal identification because personal information shared with approved companies falls outside of the scope of the statutes.\(^{234}\) The current legislation leaves consumers with little chance of judicial remedy for the unauthorized disclosure of personal information.\(^{235}\) Legislation must be enacted to broaden the scope of statutes such as the SCA to allow the court to provide judicial relief to consumers.\(^{236}\)

The Consumer Privacy Bill of Rights Act of 2014 ("2014 CPBRA"), which New Jersey Senator Bob Menendez proposed to Congress in May 2014, is a major step in the right direction.\(^{237}\) The 2014 CPBRA was read twice in the Senate, before it was ultimately referred to the Committee on Commerce, Science, and Transportation.\(^{238}\) The 2014 CPBRA, if enacted, would direct the FTC to initiate rulemaking procedures to require approved companies and data brokers to carry out security measures to protect PII,\(^{239}\) unique identifier information, and


\(^{233}\) See infra Part V.B.


\(^{235}\) See supra Part III.C.

\(^{236}\) See, e.g., Svenson, 2014 WL 3962820, at * 9.


\(^{238}\) Id.

other information that may be used to identify a specific individual. The 2014 CPBRA would also require approved companies and data brokers to do the following: notify individuals of their practices regarding the collection, use, transfer, and storage of such information; provide timely notice before implementing material change in such practices; offer consumers a mechanism to provide opt-in consent for any unauthorized use of such information or a third party's use for behavioral advertising or marketing; and provide access for consumers to their information in order that they might update it to keep it accurate.

Moreover, the 2014 CPBRA would require that notifications be clear, as many privacy agreements presently contain notifications, but they are placed at the bottom of webpages, and people rarely take the time to read them. While consumers should be proactive and seek out privacy policies before giving away their personal information, companies should have the responsibility of making this as easy as possible for the consumer.

All of these proposed changes would assist consumers in protecting their information online. If enacted, there would at last be a solid regulatory system in place for the data broker industry and the use of personal information online.

One shortfall of the 2014 CPBRA, however, is that it does not create a private right of action for consumers. For consumers to bring

and affected by the regulations. Id.

The PII referred to includes a consumers': first and last name; postal address of physical place of residence; e-mail address; telephone and mobile device number; social security number; credit card number; and biometric data. S. 2378, § 103(a)(5).

241. Id. §§ 121–122.
242. S. 2378 § 121(a); see Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 J.L. & POL’Y INFO. SOC’Y 525, 565 (2008). One study on privacy policies found they ranged in length from a low of 144 words to a high of 7669 words—that is nearly fifteen pages of text—and that it would take approximately ten minutes to read a medium length policy. McDonald & Cranor, supra, at 754. The study also asserted that a user would spend about 201 hours a year to read privacy policies from every site they visit, for a cost of about $3500 annually. Id.
243. See James Temple, Why Privacy Policies Don’t Work—and What Might, SFGATE (Jan. 29, 2012, 4:00 AM), http://www.sfgate.com/business/article/Why-privacy-policies-don-t-work-and-what-might-2786252.php (discussing the extreme time commitments to reading all privacy policies, the difficulty consumers have understanding them, and steps companies can take to remedy the problem).
246. See S. 2378, § 157; supra Part III.C. In fact, the 2014 CPBRA specifically calls for no
successful lawsuits against data collectors, a private right of action is necessary. Data itself is of great monetary value to the approved companies and to data brokers collecting and selling it, but none of that value is attributed to the consumer. Even with the implementation of an opt-in clause, litigation over breaches of privacy would be inevitable. However, if new legislation includes a private right of action allowing a civil remedy to the consumers whose personal information was improperly collected and disclosed, those consumers could achieve monetary compensation in the courts. The Ninth Circuit has already suggested that the diminished economic and proprietary value of contact information may be sufficient for a breach of contract claim, although in doing so the court held that the plaintiffs did not properly allege a market for their personal information. When crafting the new statute, lawmakers should define such a market and place a value on the data for the consumers' benefit. The statute should impose strict liability, in that if the court finds that a company has breached its duty to a consumer, it will owe a penalty to that consumer. This way, consumers will be compensated for the invasion

247. See supra Part III.C.

249. See Loewenthal, supra note 183 (explaining why privacy rules are hard to enforce in the online marketplace).
250. See White House Data Breach Legislation Must Be Augmented to Improve Consumer Protection, CDT (Jan. 16, 2015) (explaining how a private right of action works as an incentive to companies to ensure personal information is protected).
251. Svenson v. Google Inc., No. 13-cv-04080, 2014 WL 3962820, at *5 (N.D. Cal. Aug. 12, 2014) (citing In re Facebook Privacy Litig., No. 12-15619, 2014 WL 1815489, at *1 (9th Cir. May 8, 2014)). Plaintiffs are only successful in litigation over data collection after there is a data breach. See Nate Raymond, Consumers Can Sue Target Corp over Data Breach: Judge, REUTERS (Dec. 19, 2014, 10:14 AM), http://www.reuters.com/article/2014/12/19/us-target-breach-lawsuit-idUSKBNOJX1M20141219. For example, when Target suffered a breach of nearly 40 million credit card numbers and 110 million people's personal identifiable information, a judge in 2014 ruled that those who suffered harm from the breach may bring an action against Target. Id. But, if Target did not have the personal information stored or customers were able to request its removal when it is unnecessary, there would be no information to breach.
253. Such a private right of action could emulate the penalty structure found under the Telephone Consumer Protection Act ("Telephone Act"). Telephone Consumer Protection Act, 47 U.S.C. § 227 (2012). The Telephone Act allows for an action to recover for actual monetary loss for a violation of the act, or $500 for each violation, whichever is greater. § 227(5).
of their online privacy, and companies will face greater accountability for their data collection practices.\textsuperscript{254} Legislators can combine the damages of a data breach with the value of information to the companies to establish a penalty amount.\textsuperscript{255}

\section*{B. Legislation and Regulation Should Utilize Opt-In Clauses and Create a National Registry for Data Brokers}

An opt-in system will protect consumers' expectations of privacy online more so than the current opt-out structure.\textsuperscript{256} Under an opt-out system, which is currently utilized by most approved companies, consumers' personal information is shared unless they proactively and explicitly instruct the company to keep it confidential.\textsuperscript{257} Conversely, under an opt-in agreement, consumers' personal information will remain private unless they consent to its disclosure.\textsuperscript{258} Thus, under the system proposed in this Note, consumers will have to give approval before their information will be taken and used by the approved company.\textsuperscript{259} Under an opt-in system, if consumers do not read fully or do not understand a company's privacy policy, they need not worry—their information will not be shared unless they consent to do so. A presumption against disclosure would exist, which leans towards protecting privacy.\textsuperscript{260} Additionally, the new legislation should require approved companies that collect, store, and share personal information to make this presumption against disclosure clear on the website's homepage, not buried within a privacy policy.\textsuperscript{261}

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{254} See White House Data Breach Legislation Must Be Augmented to Improve Consumer Protection, supra note 250.
\item \textsuperscript{255} See Emily Steel, et al., How Much Is Your Personal Data Worth?, FIN. TIMES (June 12, 2013, 8:11 PM), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz3a3dNWmxG. While the value of individual information may be low, it is multiplied greatly when a broker sells the information to many companies. See Singer, supra note 252.
\item \textsuperscript{256} See Hatch, supra note 142, at 1494-95.
\item \textsuperscript{257} See id.
\item \textsuperscript{258} See id.
\item \textsuperscript{259} Companies have been known to collect personal information without giving consumers' the knowledge they can opt out. See, e.g., Hunton & Williams LLP, FCC Announces 7.4 Million Dollar Settlement with Verizon, HUNTION PRIVACY BLOG (Sept. 5, 2014), https://www.huntonprivacyblog.com/2014/09/articles/fcc-announces-7-4-million-dollar-settlement-verizon/#more-6425 (discussing the circumstances in which the Federal Communications Commission settled with Verizon after an investigation into the telecommunications company's use of personal information for marketing). A federal investigation revealed that Verizon had used customers' personal information for marketing purposes over a multiyear period before notifying customers of their right to opt out of such marketing. Id.
\item \textsuperscript{260} See Hatch, supra note 142, at 1494.
\item \textsuperscript{261} See Be Transparent: Give Users the Ability to Make Informed Choices, ACLU, http://aclunc-tech.org/primer/privacy/be-transparent (last visited Sept. 2, 2015).
\end{enumerate}
\end{footnotesize}
Opt-in clauses will also further the goals of lawmakers and administrators to force approved companies and data brokers to make their policies more clear and transparent. Companies want consumers to share their personal information; thus, they should provide a clear opt-in procedure in order to ease consumer concerns about privacy and get more consumers to do so. But, this will only be successful if the policy requirements set forth by statute promote clear and concise privacy policy contents, and companies are held accountable if the requirements are not met. New opt-in clauses should aim to better inform consumers about the company’s data collection practices in accordance with government requirements and recommendations, and ensure that consumers’ personal information will not be shared without their consent.

Currently, when users log on to Target’s online shopping center, privacy is far from the main focus of the webpage. Visitors must scroll to the bottom of the page to find a diminutive link to the company’s privacy policy. When users look through the privacy policy, they are presented with the ways in which Target collects consumers’ personal information, the types of information collected, and how Target uses that information. The more unassuming uses are placed first—fraud prevention, internal marketing, internal operations, compliance, etc. Once users scrolls down, however, they will notice that Target also shares personal information with third parties for marketing. Target assumes users agree to this use, and if they do not want their information used for this purpose, consumers must actively “opt-out.” Thus, if

262. See Fed. Trade Comm’n, supra note 20, at 5, 46. Transparency was a key focus in the FTC’s recommendations to Congress for legislation regarding the data broker industry. Id.
263. See Hatch, supra note 142, at 1497.
264. Id. at 1499-500.
265. See supra notes 267-80 and accompanying text.
266. See Hatch, supra note 142, at 1494-95.
268. Id. Generally all approved companies place their privacy policy on the webpage’s footer. See Where to Place Privacy Policy on Your Website, TERMSFEED (Nov. 8, 2013), https://termsfeed.com/blog/where-place-privacy-policy-website.
270. Id.
271. Id. The notice is offered not so much to inform the consumer, but rather to protect Target from liability under state disclosure laws. See Clark D. Asay, Consumer Information Privacy and the Problem(s) of Third-Party Disclosures, 11 NW. J. TECH. & INTELL. PROP. 322, 344 (2013); see also CAL. BUS. & PROF. CODE § 22575(b).
272. Privacy Policy, supra note 26. The privacy policy states that users can opt-out of the sharing of personal information with third parties. Id. However, Target makes sure to not place an active hyperlink directly in the choices for an opt-out section, which would facilitate the opt-out for
consumers do not review the privacy policy in full, or merely do not exercise their opt-out option, their information will be shared with third-parties without their knowledge. Utilizing an opt-in approach to the third-party sharing is a solution to the current system that leans toward informed disclosure.

Furthermore, opt-ins would be most effective if provided in a pop-up that appears when consumers first log on to an approved company’s webpage, because information may be gathered without even manually entering it. Target specifies in its privacy policy that it collects browsing information through cookies and, in doing so, it automatically collects personal information. Target and its service provider use not only cookies, but also “web beacons, and other technologies to receive and store certain types of information,” such as pages visited on the website, a user’s web address, purchase information, and check out procedures, among others. This information is not just kept internally—it is shared with third-party marketers. The law should instead require that when consumers visit a webpage that conducts data collection and third-party sharing, a notice instantly comes up. This notice could read as follows:

NOTICE: TARGET WOULD LIKE TO COLLECT AND SHARE YOUR PERSONAL INFORMATION WITH THIRD-PARTY MARKETING COMPANIES FOR YOUR BENEFIT. TARGET WILL NOT USE YOUR INFORMATION WITHOUT YOUR CONSENT. CLICK HERE TO CONSENT TO THIS USE. FOR A

consumers. Instead, users must continue to scroll down even further, and then click on a link where they must enter their information in order to opt out. That section is not labeled “opt-out,” but rather “what choices you have.” In addition, the policy does not specifically state what personal information is shared with third parties, or who those third parties are.

See Jacqueline Emigh, Note to Facebook on Privacy: How About Opt-In, Not Opt Out?, PCWORLD (May 25, 2010, 12:25 AM), http://www.pcworld.com/article/197060/Facebook_Privacy.html. Under an opt-in system, the default will be to not share personal information, allowing consumers to have more control over the data collection process. See id.

See Buzzit Media, Benefits of Pop-Ups, HUBPAGES, http://buzzit-media.hubpages.com/hub/popup-review (last updated June 21, 2013). A pop-up window will attract the attention of the user, as opposed to an inconspicuous link to a privacy policy at the bottom of the homepage. See id.

Privacy Policy, supra note 26. Cookies are small files a web server automatically collects that are stored as text files and contain information such as login and usernames, passwords, shopping cart information, preferences, among others. Cookies, NETLINGO, http://www.netlingo.com/word/cookies.php (last visited Sept. 2, 2015).

LIST OF THE MARKETING COMPANIES AND THEIR USE OF YOUR PERSONAL INFORMATION, CLICK HERE.

With such a notification, users’ information cannot be automatically shared—it may be shared only with users’ affirmative consent. Additionally, hyperlinks should be included under the headings “Marketing Companies” and “For Your Benefit.” These links should direct consumers to a webpage containing the names of the data brokers or other similar companies with which consumer information might be shared and a webpage containing the data companies’ privacy policies, describing for what purpose exactly the information is being shared. Such a notification would help make it abundantly clear to consumers which companies will share their personal information, would provide an easily accessible location where they have an opportunity to review the uses of their information, and would allow consumers to provide actual informed consent.

While an opt-in approach will allow consumers to control whether or not their information is shared, there still remains the problem of controlling information that has already been shared. There are

280. See Hatch, supra note 142, at 1498-99. It has been argued that “opt-out” takes an opposite approach to contract law by allowing silence to be deemed as consent. Id. at 1498. The idea is that under ordinary contract law silence is not deemed consent, as both parties must affirmatively agree to make a contract. See id. However, with opt-out agreements, silence is regarded as consent. Id. A consumer’s silence (by not opting out) transforms into an acceptance of a company’s information sharing practices. Id. Opt-in agreements, conversely, allow the consumer the opportunity to affirmatively consent to the company’s collection practices, and allows for greater freedom to accept or reject the policy. Id. at 1498-99. Therefore, under an opt-in system, consumers have greater control over their data. Id.


282. A major concern of government officials and those in the private sector, alike, is the lack of information as to what data brokers do with consumers’ personal information. See FED. TRADE COMM’N, supra note 20, at 6-7.

283. By having to opt-in, consumers will be sure they are not tracked online and their personal information stored without their knowledge. See Data: Getting to Know You, ECONOMIST (Sep. 13, 2014), http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party. As it stands now, Target’s privacy policy is vague in their description of third-party uses, stating only that “[t]hese companies ... may use the information ... to provide special offers and opportunities.” Privacy Policy, supra note 26. To conform to California state law, the privacy policy informs consumers that they can contact Target to receive a notice of the information that was shared with third parties in the past year. See CAL. BUS. & PROF. CODE § 22575(b)(1)-(3); see Privacy Policy, supra note 26. However, under the current terms, consumers must physically mail Target a form and wait for a response just to see with whom their information was shared. Privacy Policy, supra note 26.

284. Target, for example, states in their privacy policy only that they share consumers’ information with “third parties,” but does not reveal who these third parties are. Privacy Policy,
hundreds of data broker companies that already have troves of consumers’ personal information.\textsuperscript{285} Many of these companies, as mentioned above, exist largely unknown to the public.\textsuperscript{286} Furthermore, it is difficult to obtain information from data broker companies regarding the type of information they collect, how they collect it, and how they store it.\textsuperscript{287}

Each of these issues could be solved by the creation of a data broker registry—a platform where data broker companies are listed, and consumers can view privacy policies for each and opt out from any company’s collection practices.\textsuperscript{288} With such a registry, consumers could also see what information has been collected and request that the information that is not being actively used, or used for a purpose they do not want, be deleted permanently.\textsuperscript{289} Likewise, regardless of whether the consumer chooses to have the information deleted, the information should be stored for a fixed term necessary for its use, not indefinitely.\textsuperscript{290}

The FTC has been advocating for such a registry.\textsuperscript{291} In its report to Congress on data brokers, the FTC advocated for a centralized portal “where data brokers can identify themselves, describe their information collection and use practices, and provide links to access tools and opt outs.”\textsuperscript{292} A registry of this nature would certainly be beneficial in helping users identify, and perhaps control, the information collected and shared about them by data broker companies.\textsuperscript{293} Any legislation would also have to include a penalty for data brokers that do not register on the website to incentivize registration.\textsuperscript{294}


\textsuperscript{286.} See Beckett, supra note 285; supra Part I.A.

\textsuperscript{287.} See id. In a study, researchers from the University of California at Berkley reached out to data brokers for information, but most refused. \textit{id.} Data companies typically will not reveal the exact companies that sell them information, and retailers make it difficult to find out whether they are selling information. \textit{id.}


\textsuperscript{289.} For a description of the types information data brokers possess, see Beckett, \textit{supra} note 285.

\textsuperscript{290.} \textit{See Fed. TRADE COMM’N, supra} note 20, at 22.

\textsuperscript{291.} \textit{id.} at 50.

\textsuperscript{292.} \textit{id.}

\textsuperscript{293.} \textit{id.} at 50-53.

\textsuperscript{294.} As an example of such system, under the Telephone Act, if a seller or telemarketer places a telemarketing call when they have not accessed the registry or paid its fees, they may be subject to fines up to $16,000 per violation. \textit{Q&A for Telemarketers & Sellers About DNC Provisions in TSR, FED. TRADE COMMISSION}, http://www.ftc.gov/tips-advice/business-center/qa-telemarketers-sellers-
While there are privately-held websites containing data broker information and opt-outs, these websites are not overly effective because the list of brokers is not exhaustive—there is no incentive for data brokers to register on these private websites. The registry should also require data brokers to include a detailed description of the type of information each data broker possesses, where they received the information, and how exactly they use it. Similar legislation exists in the consumer protection context, with similar requirements governing consumer reporting. Pursuant to the Fair Credit Reporting Act, credit reporting agencies must show consumers upon their request free copies of their credit reports and let them correct any errors. The data broker registry could include a similar provision, requiring data brokers to issue reports to consumers containing the personal information each broker has on file, so consumers could keep that information accurate and gain more control over the collection and dissemination of their personal information.

In addition to a comprehensive list of data brokers and their respective privacy policies and use of information, the registration portal should also include an option for consumers to opt out of all data collection and storage. This way, consumers would need not go through the cumbersome task of opting out from each potential data broker using their information. A similar system exists with the National Do Not Call Registry that was created under the Telephone Consumer Protection Act of 1991. Under that system, people can register their phone number on the registry, which in turn bars

295. See, e.g., STOP DATA MINING, http://www.stopdatamining.me (last visited Sept. 2, 2015). StopDataMining.me’s goals are to be the central source where consumers learn what kinds of information data brokers have about them and how to exercise their opt-out choices and to act as the “Do Not Call” list for data broker companies. Our Mission, STOP DATA MINING, http://www.stopdatamining.me/our-mission (last visited Sept. 2, 2015).

296. For example, personal data can be used for targeted advertising and marketing to individuals’ needs and desires, or used for security verification purposes. Morris & Lavandera, supra note 104.


298. Id. § 1681(g)–(i); see Free Credit Reports, FED. TRADE COMMISSION, http://www.consumer.ftc.gov/articles/0155-free-credit-reports (last visited Sept. 2, 2015).

299. See FED. TRADE COMM’N, supra note 20, at 50-53.

300. Currently, there are private websites that compile lists of data brokers, and include links to their privacy policies and opt out agreements. See Data Broker Opt-Out List, supra note 288. However, you must click on each individual broker, and there are hundreds. Id.

301. See id.

telemarketers from contacting them at their registered numbers. In the registry system proposed by this Note, consumers could register their email addresses and names to restrict brokers from collecting and storing their personal information, and from sending spam marketing emails and messages on social media.

In addition, the Do Not Call registry requires solicitors to provide their names, names of the people or entities on behalf of whom the call is made, and a telephone number or address for that person or entity. Data brokers should be required to notify a consumer when they collect or purchase personal information, and the data broker, like telemarketers on the Do Not Call Registry, would then have to provide information about who they are, where they are located (both physically and on the Internet), what information they are collecting, and what they will do with that information.

V. CONCLUSION

Opt-in provisions are the best way to ensure that consumers’ privacy expectations are met. Should the legislature adopt a mandatory opt-in approach to consumer consent, the default position on data sharing will be switched from sharing personal information to not sharing. Additionally, until the legislature provides a clear statute giving consumers a private right of action for invasion of privacy through unauthorized use of personal data and putting a monetary value on that data, consumers will continue to have difficulty in receiving judicial remedies due to a failure to adequately plead damages. Lastly, the data broker market needs to be far more transparent—consumers should have absolute control over their personal information. The United States is behind the times with data collection protection in comparison to the rest of the world, and it is time to catch up.

304. Id. § 227.
305. Id. § 227(b)(2)(E).
306. See id.
307. See supra Part IV.B.
308. See supra Part IV.B.
309. See supra Part IV.A.
310. See supra text accompanying notes 288-311.
311. See Protection of Personal Data, EUR. COMMISSION ON JUST., http://ec.europa.eu/justice/data-protection (last visited on Sept. 2, 2015). For example, European Union ("EU") law imposes strict conditions to be satisfied for companies seeking to gather and deal in personal data, including proving a legitimate purpose. Id. Additionally, those who collect and share your information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law. Id.
consumer privacy protection will be advantageous to consumers and companies alike, because consumers will want to do more business with those companies that they can trust.  

Eugene E. Hutchinson*