

## Notes

### Someone is Watching: The Need for Enhanced Data Protection

NIC ROETHLISBERGER\*

*The computer revolution has created a world where communication is cheap and instantaneous, and where vast amounts of information and consumer goods are just a click away. It also has created a world where the electronic gadgets we use every day create a trail of information that is being collected, examined, sold, and—far too often—stolen. Individuals have little to no control over the use and sale of this personal, private information, and the law has failed to keep pace. Some privacy advocates have suggested that traditional privacy torts should be used by the courts to stop the worst of these privacy invasions. However, these torts, developed more than fifty years ago, are ill-suited to the task. In addition, many states and the federal government have passed laws and regulations to protect the most sensitive of private information from prying eyes. But these laws have proven to be inadequate in a rapidly changing world of iPhones, Netflix, and Internet searches. What is needed is a national standard that will protect the privacy of individuals without stifling innovation. A ban on the dissemination of private information, along with more stringent laws meant to prevent identity theft, will go a long way to achieving these twin goals.*

---

\* J.D., University of California, Hastings College of the Law, 2011; B.A., San Francisco State University, 2004. I would like to thank to my wife, Dhyana Levey, for her help and patience through the process of writing this Note, and for the gift of our baby girl, Audrey Roethlisberger. I would also like to thank Professor John Diamond for his early suggestions and the San Francisco Giants for making my last year of law school bearable.

## TABLE OF CONTENTS

INTRODUCTION.....	1794
I. THE PRIVACY TORTS.....	1798
A. INTRUSION UPON SECLUSION .....	1799
B. PUBLIC DISCLOSURE OF PRIVATE FACTS.....	1801
C. APPROPRIATION .....	1804
II. BREACH OF CONFIDENTIALITY .....	1807
A. THE CONTRACT THEORY .....	1809
B. THE FIDUCIARY RELATIONSHIP THEORY .....	1811
C. CREATING A TORT.....	1814
III. INFORMATION AS A PROPERTY RIGHT .....	1815
IV. THE CURRENT STATE OF STATUTORY AND REGULATORY LAW.....	1816
A. FEDERAL LAW .....	1817
1. <i>Financial Information</i> .....	1817
2. <i>Information-Specific Statutes</i> .....	1818
3. <i>Other Federal Laws</i> .....	1819
B. ADMINISTRATIVE LAW .....	1820
C. STATE LAWS .....	1821
1. <i>Notification Laws</i> .....	1821
2. <i>Disposal and Minimum Security Statutes</i> .....	1823
3. <i>Financial Information Statutes</i> .....	1824
4. <i>Internet-Specific Legislation</i> .....	1824
V. WORKING TOWARD A SOLUTION.....	1825
A. DATA COLLECTION .....	1826
B. INTERNAL DATA USE.....	1827
C. INFORMATION SALE AND RENTAL.....	1829
D. DATA THEFT.....	1831
E. A CONSTITUTIONAL LIMITATION .....	1833
F. COMPETING PROPOSALS.....	1834
1. <i>Do Not Track</i> .....	1835
2. <i>Privacy Bill of Rights</i> .....	1836
CONCLUSION .....	1838

## INTRODUCTION

Whenever you visit a website, buy a book, shop for groceries, conduct a Google search, buy a magazine, or vote in an election, a person or software program is likely watching—and making note of your activities. A surprising amount of information about you is stored in private databases, and that information is not just collecting digital dust. This data is being used by the company that collected it, and is often

aggregated with other information about you and then sold. And, sometimes, it's stolen.<sup>1</sup>

Commercial data collection is nothing new. Companies have been exploiting data for sales and research purposes for decades.<sup>2</sup> However, in the last few decades, this data collection has become big business. Firms collect mountains of data and assemble what Daniel Solove calls “digital dossiers,”<sup>3</sup> which contain a large amount of seemingly private information including Social Security numbers, date of birth, household income, health information, occupation, book preferences, religion, and dress size.<sup>4</sup> The storage and use of this information has become a major profit center for businesses, and for some, this data is the most important asset they own.<sup>5</sup>

A recent *Wall Street Journal* investigation of the fifty most popular websites found that all of them—except the nonprofit site Wikipedia—install “intrusive consumer-tracking” software on the computers of those who visit the sites.<sup>6</sup> Two thirds of the files installed on the user's computer, often without their knowledge, came from companies that exist solely to collect the information of Internet users.<sup>7</sup> And the tracking goes far beyond merely recording the websites that a person visits. Some files record keystrokes; others “can re-spawn” after they have been deleted.<sup>8</sup>

---

1. A recent survey on identity fraud found that 4.8% of the U.S. population has suffered from fraud. See RITA TEHAN, DATA SECURITY BREACHES: CONTEXT AND INCIDENT SUMMARIES (2008), for a list of recent data losses; see also *Chronology of Data Breaches: Security Breaches 2005–Present*, PRIVACY RIGHTS CLEARINGHOUSE (Apr. 15, 2011) <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (providing a continually updated list of data losses and breaches).

2. See DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 16–17 (2006) (discussing that as early as the 1920s, General Motors used information on Ford customers to entice them to buy a General Motors vehicle); ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY 3–5 (1972).

3. SOLOVE, *supra* note 2, at 1.

4. *Privacy and Consumer Profiling*, ELECTRONIC PRIVACY INFORMATION CENTER, <http://epic.org/privacy/profiling> (last visited July 4, 2011). Collected information is then sifted and sorted to place people into categories sold to marketers. For example, Claritas, one company that collects data and uses it to create “dossiers” on individuals, divides people into fifteen categories with whimsical names like “Landed Gentry.” These categories are further broken down into subcategories. Landed Gentry is divided into “Country Squires,” “God's Country,” “Big Fish Small Pond,” and “Greenbelt Families.” *Id.*

5. CHARLES H. KENNEDY, THE BUSINESS PRIVACY LAW HANDBOOK 1 (2008); see Steve Lohr, *Data Explosion Remakes Retailing*, N.Y. TIMES, Jan. 3, 2010, at BU3. Lohr's article discusses how retailers use “internal sources including point-of-sale and shipment-tracking information, as well as census data and syndicated services” to improve their ability to target customers. Additionally, Lohr shows that retailers “also track online visitors to Web commerce sites, members of social networks like Facebook and browsers using smartphones.” *Id.*

6. Julia Angwin and Tom McGinty, *Personal Details Exposed via Biggest U.S. Websites*, WALL ST. J., July 31, 2010, at A1.

7. *Id.*

8. *Id.*

The technology that facilitates this tracking is only getting better. New technologies are increasing the amount and detail of data that can be collected. For example, the new web-browsing standard, HTML 5, will allow for increased tracking and data collection.<sup>9</sup> Smartphones are also becoming a major worry for privacy advocates. An investigation into the 101 most popular smartphone applications showed that fifty-six of them transmitted the phone's unique user ID number, which cannot be changed.<sup>10</sup> A further forty-seven transmitted the phone's location and five sent age, gender, and other personal information to outside vendors.<sup>11</sup>

Companies use this data in three ways, each with its own particular privacy concerns. First is the collection of data. This can include simply requesting information at the point of customer contact or seeking out the information in places such as public records. But the Internet and smartphones allow companies to go far beyond these rudimentary data-collection techniques. Second is the in-house use of that data. Many companies collect their own customer information and use it for their business needs. Amazon.com is a good example: The online shopping site uses customers' purchasing data to make product recommendations and improve search capabilities.<sup>12</sup>

Finally, and most worryingly, companies sell this data to third parties.<sup>13</sup> This activity is particularly disturbing because a company with which the consumer has no relationship, and that they may never have heard of, has access to vast amounts of her personal information. Indeed, by 1995 there were already five database compilers with data on almost every household in the United States.<sup>14</sup> The Internet enables companies to sort and combine information in ways never before possible.<sup>15</sup> This

---

9. Tanzina Vega, *Web Code Offers New Ways to See What Users Do Online*, N.Y. TIMES, Oct. 11, 2010, at A1; see also Jessica E. Vascellaro, *Suit to Snuff Out "History Sniffing" Takes Aim at Tracking Web Users*, WALL ST. J., Dec. 6, 2010, at B1 (showing that some websites use "history sniffing" to figure out what other sites the visitor has gone to); Tanzina Vega, *Code That Tracks Users' Browsing Prompts Lawsuits*, N.Y. TIMES, Sept. 21, 2010, at B3.

10. See ERIC SMITH, *IPHONE APPLICATIONS & PRIVACY ISSUES: AN ANALYSIS OF APPLICATION TRANSMISSION OF IPHONE UNIQUE DEVICE IDENTIFIERS (UDIDs)* (2010); Scott Thurm and Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J., Dec. 18, 2010, at C1.

11. Thurm, *supra* note 10, at C1.

12. See Laurie J. Flynn, *Like This? You'll Hate That (Not All Web Recommendations Are Welcome)*, N.Y. TIMES, Jan. 23, 2006, at C1.

13. The Federal Trade Commission (FTC) has a helpful graphical representation showing how personal data is collected and distributed to data brokers who then deliver the data to entities who use it for a wide range of purposes. *Personal Data Ecosystem*, FTC, <http://www.ftc.gov/bcp/workshops/privacyroundtables/personalDataEcosystem.pdf> (last visited July 4, 2011); see also FTC, *STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING* (2009) [hereinafter *FTC STAFF REPORT*].

14. ARTHUR M. HUGHES, *THE COMPLETE DATABASE MARKETER* 354 (1996).

15. See generally *FTC STAFF REPORT*, *supra* note 13.

includes the ability to track online behavior and tailor advertising to fit with websites recently visited by the user.<sup>16</sup> For example:

[T]he information about the consumer's activities on [a] travel website could be combined with information about the content that the consumer viewed on [a] newspaper's website. The advertisement served could then be tailored to the consumer's interest in, not just New York City, but also baseball (*e.g.*, an advertisement referring to the New York Yankees).<sup>17</sup>

The fact that this information is falling into many different hands with varying levels of protection inevitability leads to another major privacy concern: data loss. Sometimes data is lost through carelessness, and sometimes it is stolen by those who hope to exploit it for criminal gain. Because of the sheer volume of information maintained by some companies, one incident can expose millions of people to identity theft. In June 2005, credit card processing company CardSystems Solutions, Inc. admitted to one of the largest data breaches in history.<sup>18</sup> About forty million cardholders' credit card information was stolen when the company's computer systems were breached. More recently, a 28-year-old college dropout was convicted of stealing information from more than 130 million credit and debit cards by hacking into the computer systems of retailers such as 7-Eleven.<sup>19</sup>

This Note will concentrate on legal academics' attempts to address these problems through common law torts, the current state of the relevant statutory and administrative law, and why further action by Congress is the best solution to the problems posed by data collection, use, sale, and theft. Creating straightforward, easily implemented rules that safeguard the public from the most worrisome of violations, while protecting the profits of industries that are increasingly driving positive innovation, should be the goal. Part I discusses the failure of privacy tort law to address these issues. Part II argues that a cause of action for breach of confidence should not be extended to cover dissemination of private information. Part III explains why creating a property right in personal information would conflict with basic ideas of intellectual property. Part IV discusses the current state of statutory and administrative law at both the federal and state level. Finally, Part V proposes that extending current law is the best way to prevent the worst invasions of privacy.

---

16. *Id.*

17. *Id.* at 3. One version of this technique is called "retargeting" or "remarketing," where a particular item viewed online follows the consumer around through display ads, encouraging her to go back and buy it. Miguel Helft & Tanzina Vega, *Seeing That Ad on Every Site? You're Right. It's Tracking You*, N.Y. TIMES, Aug. 30, 2010, at A1.

18. Eric Dash, *Lost Credit Data Improperly Kept, Company Admits*, N.Y. TIMES, June 20, 2005, at A1.

19. Donna Goodison, *Decade of Lost Identities*, BOSTON HERALD, Dec. 26, 2009, at 19.

## I. THE PRIVACY TORTS

Some scholars have advocated the use of the traditional privacy torts as a solution to the data collection and trading problem. The traditional beginning of modern privacy protection in the United States stems from Samuel Warren and Louis Brandeis's *The Right to Privacy*, published in 1890.<sup>20</sup> Called the most influential law review article ever written,<sup>21</sup> it laid the foundation for modern privacy law by asking that courts begin to enforce new privacy torts so that people would have the right "to be let alone."<sup>22</sup> By 1960, the right to privacy in some form was recognized in the vast majority of states.<sup>23</sup> At that time, William Prosser distilled the mountain of privacy jurisprudence developed over the preceding seventy years into the four torts now recognized by modern courts:<sup>24</sup> intrusion upon seclusion,<sup>25</sup> public disclosure of private facts,<sup>26</sup> false light,<sup>27</sup> and appropriation of likeness.<sup>28</sup>

Unfortunately, these torts do "little to protect against the collection, use, and dissemination" of personal information.<sup>29</sup> As discussed below, this is because the three torts most likely to be of use in these situations—intrusion upon seclusion, public disclosure of private facts and misappropriation—have serious limitations.<sup>30</sup> While there are indications that courts may be willing to use the intrusion upon seclusion tort in cases involving spyware,<sup>31</sup> it is unlikely to be applied more broadly because in most circumstances the user is giving up the information voluntarily. Similarly, limitations on the public disclosure tort make it difficult to use in all but the most extreme violations of privacy. The tort has also come under more fundamental attack for being almost certainly unconstitutional.<sup>32</sup> Of the four privacy torts, appropriation is the most

---

20. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

21. Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966).

22. Warren & Brandeis, *supra* note 20, at 195.

23. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 386–88 (1960).

24. *Id.* at 389.

25. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

26. *Id.* § 652D.

27. *Id.* § 652E.

28. *Id.* § 652C.

29. Robert Sprague & Corey Ciochetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 112 (2009).

30. The false light tort is unlikely to be of much use because it protects against information that portrays someone in a false way. With databases, however, it is the accuracy of the information that is the problem, not its falsity. See Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 165–66 (2006).

31. See Don Corbett, *Virtual Espionage: Spyware and the Common Law Privacy Torts*, 36 U. BALT. L. REV. 1, 24–31 (2006) (discussing how a plaintiff might successfully argue a claim of intrusion upon seclusion against the user of spyware).

32. Erwin Chemerinsky, *Protecting Truthful Speech: Narrowing the Tort of Public Disclosure of Private Facts*, 11 CHAP. L. REV. 423, 424–26 (2008). Even the Restatement (Second) of Torts contains a

likely to protect against some of the activities of database managers, but it too is almost certain to fail.<sup>33</sup>

#### A. INTRUSION UPON SECLUSION

The tort of intrusion upon seclusion protects against the invasion of personal space, as well as the interest in solitude and seclusion.<sup>34</sup> The tort of public disclosure of private facts, on the other hand, protects against the unauthorized disclosure of facts and has little to do with how those facts were obtained.<sup>35</sup> This distinction makes intrusion upon seclusion most relevant in the collection of database information, rather than in the use, sale, or theft of the information.

The intrusion tort requires four elements: (1) The invasion must be intentional, (2) the matter intruded upon must be private, (3) the intrusion must be highly offensive to a reasonable person, and (4) the intrusion must cause anguish and suffering.<sup>36</sup> These elements create significant hurdles to maintaining a cause of action against a company for collecting personal information. In particular, the requirements that the intrusion be into a private matter and that it be “highly offensive” to a reasonable person create almost insurmountable barriers.

The private matter requirement is strictly enforced, and a plaintiff must prove that she had a reasonable expectation of privacy.<sup>37</sup> The comments to the Restatement (Second) show that there is no liability for giving further publicity to what the plaintiff leaves open to the public.<sup>38</sup> The question is how the information was collected, not necessarily what the information is.<sup>39</sup> Merely aggregating information voluntarily given to a company would not be covered by this tort, and collecting information about what one does in public—such as buying groceries, voting, putting something up on Facebook, or simply the location of a person in public—is almost certainly not covered.

For example, in *Dwyer v. American Express Co.*,<sup>40</sup> American Express cardholders filed a class action lawsuit against the credit card company alleging invasion of privacy. American Express was renting out

---

warning about the potential unconstitutionality of the tort. See RESTATEMENT (SECOND) OF TORTS § 652D special note (1977) (“It has not been established with certainty that liability of this nature is consistent with the free-speech and free-press provisions of the First Amendment to the Constitution, as applied to state law.”).

33. See Ludington, *supra* note 30, at 166–71.

34. *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 494 (1975); see Prosser, *supra* note 23, at 389.

35. RESTATEMENT (SECOND) OF TORTS § 652B cmt. a (1977).

36. *Snakenberg v. Hartford Cas. Ins. Co.*, 383 S.E.2d 2, 6 (S.C. Ct. App. 1989); RESTATEMENT (SECOND) OF TORTS § 652B (1977).

37. *Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 490 (Cal. 1998).

38. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).

39. However, the type of information collected could have a bearing on the “highly offensive” requirement.

40. 652 N.E.2d 1351 (Ill. App. Ct. 1995).

information on its customers' spending habits.<sup>41</sup> Specifically, the action sought damages on a theory of intrusion upon seclusion.<sup>42</sup> But the Appellate Court of Illinois held that the company's actions did not involve intrusion into a private matter.<sup>43</sup> The court reasoned that

By using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.<sup>44</sup>

The court in *Dwyer* favorably cited *Shibley v. Time, Inc.*<sup>45</sup> In *Shibley*, the Court of Appeals of Ohio held that magazine publishers were not liable for selling their subscriber information to direct mail advertisers.<sup>46</sup>

The requirement that the intrusion be highly offensive also makes it unlikely that a court would allow a claim of intrusion upon seclusion. The law protects objectively normal sensibilities, not subjectively heightened sensitivity.<sup>47</sup> This element also requires that the intrusion cause "mental suffering, shame, or humiliation to a person of ordinary sensibilities."<sup>48</sup> It is difficult to argue that simple collection of information freely given to a company would amount to something so "highly offensive" to a reasonable person. The key to this element is that the intrusion is not just unpleasant or something people would rather avoid, but highly offensive. This requirement is a major obstacle for any plaintiff alleging intrusion for collecting the kind of information found in most databases:<sup>49</sup> "Each particular instance of collection is often small and innocuous; the danger is created by the aggregation of information, a state of affairs typically created by hundreds of actors over a long period of time."<sup>50</sup>

It is also relevant that the more common an activity becomes—and the more the population accepts the practice—the less likely it is that a court would find such an activity to be highly offensive:<sup>51</sup> "The reasonable

---

41. Albert B. Crenshaw, *Credit Card Holders to Be Warned of Lists*, WASH. POST, May 14, 1992, at D11 ("American Express segments its card holders into six tiers, ranging from the least affluent, 'value-oriented' customers to the most affluent, which it calls 'Rodeo Drive Chic.'").

42. *Dwyer*, 652 N.E.2d at 1353.

43. *Id.* at 1354.

44. *Id.*

45. *Id.* at 1355 (citing *Dwyer v. Am. Express Co.*, 341 N.E.2d 337 (Ohio Ct. App. 1975)).

46. *Id.* at 339.

47. RESTATEMENT (SECOND) OF TORTS § 652A (1977).

48. *McGuire v. Shubert*, 722 A.2d 1087, 1092 (Pa. Super. Ct. 1998).

49. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1432 (2001).

50. *Id.* (citing *Tureen v. Equifax, Inc.*, 571 F.2d 411, 416 (8th Cir. 1978) (holding that obtaining past insurance history is not tortious); *Seaphus v. Lilly*, 691 F. Supp. 127, 132 (N.D. Ill. 1988) (obtaining a person's unlisted telephone number); *Shibley*, 341 N.E.2d at 339 (obtaining magazine subscription lists)).

51. *See Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 490 (Cal. 1998) (holding that a camera

person standard incorporates society's expectations of what matters should be protected as private."<sup>52</sup> And as social expectations change, so too does what is considered to be highly offensive.<sup>53</sup> "[C]ourts define privacy by reference to society's prevailing understanding of what is a reasonable expectation of privacy. Because this conception of privacy tracks societal expectations, what is protected as private will vary in accordance with relevant social changes."<sup>54</sup>

A recent study sought to gauge public opinion on the collection of private web-surfing information for use in targeted advertising, an activity that worries privacy-rights activists.<sup>55</sup> The data indicate that a strong majority of people do not want advertising targeted at them.<sup>56</sup> The number of those who are "not OK" with targeted advertising rises from sixty-six percent to seventy-three percent when they are told the information for the targeting came from the website they were visiting.<sup>57</sup> This is a classic in-house use of private data. However, even though three-fourths of the population might be uncomfortable with use of in-house information for targeted advertising, that does not make it highly offensive. Other consumers have noted that they actually like some of the most invasive tracking as it allows them to see ads and products tailored to their personal interests.<sup>58</sup> And as the practice of collecting information from customers becomes more common, courts are unlikely to find the practice to be highly offensive.

The problems with establishing that the activities intrude on a private sphere, that the intrusion was highly offensive, and that the activities rise to the level of an intrusion at all, seem to be almost insurmountable bars to using the intrusion tort in the collection of private information.

## B. PUBLIC DISCLOSURE OF PRIVATE FACTS

The tort of public disclosure of private facts protects against the disclosure of private information. This is unlike the tort of intrusion upon seclusion, which protects people from the intrusion into their private lives in the first place. This tort would most likely be used to stop the sale

---

crew following the usual practices of the journalism business was not liable for intrusion upon seclusion because the public should expect a camera crew to film an accident scene and therefore doing so was not highly offensive).

52. Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 853 (2002).

53. *See id.* at 846.

54. *Id.*

55. JOSEPH TUROW ET. AL, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT (2009).

56. *Id.* at 3 (finding that sixty-six percent of those surveyed said they would not like websites to display advertising targeted to their interests).

57. *Id.*

58. FTC STAFF REPORT, *supra* note 13, at 9–10.

or other dissemination of private information. It would be of little use, however, in preventing the collection of the information itself or of the accidental loss or theft of the information.

The tort can be broken down into four elements: (1) the information must be given publicity, (2) the information must concern “the private life of another,” (3) its disclosure must be “highly offensive to a reasonable person,” and (4) the information must not be of “legitimate” public concern.<sup>59</sup> Just as with the intrusion tort, the disclosure tort has serious limitations when dealing with information that is only somewhat private. Much of the information in commercial databases might seem private but when examined more closely is actually “public.” A person’s address, phone number, age, hobbies, marital status, and so forth are all in the public sphere and therefore are not “private” as defined by the disclosure and seclusion torts. Similarly, the disclosure tort requires that the disclosure be “highly offensive” to a reasonable person. This element of the tort runs into problems similar to those encountered with the intrusion tort.<sup>60</sup> However, there are two problems with the disclosure tort that are not present in the intrusion tort: one related to publicity and one related to the First Amendment.

The first problem unique to this tort is the requirement that the information be given publicity. While not specifically defined, it is a more difficult standard for a plaintiff to meet than the “publication” requirement in the area of defamation, which only requires that the information be provided to a third person.<sup>61</sup> Most likely, this tort is limited to widespread dissemination of information to the public at large, or at least to a number of individuals.<sup>62</sup> The “publicity” requirement would likely not be satisfied if the information never left the organization that collected it or were shared with a few third parties.<sup>63</sup> However, the requirement could possibly be met if the information were shared widely enough through the sale<sup>64</sup> or was released to the public at large.<sup>65</sup>

---

59. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

60. See *supra* Part I.A, describing problems with the intrusion tort.

61. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977). This is in contrast to the tort of defamation, which requires only “publication” of the matter “to one other than the person defamed.” *Id.* § 577(1).

62. Solove, *supra* note 49, at 1433 (“Although this tort could conceivably be applied to certain uses of databases, such as the sale of personal information by the database industry, the tort of private facts appears designed to redress excesses of the press, and is accordingly focused on the widespread dissemination of personal information in ways that become known to the plaintiff.”).

63. *Peterson v. Idaho First Nat’l Bank*, 367 P.2d 284, 288 (Idaho 1961) (holding that a bank sharing a customer’s private financial information with a third party did not satisfy the publicity requirement).

64. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977) (“[I]t is not an invasion of the right of privacy, within the rule stated in this Section, to communicate a fact concerning the plaintiff’s private life to a single person or even to a small group of persons.”).

65. A recent class action lawsuit filed in the Northern District of California against Netflix illustrates the possible use of the public disclosure tort. See Complaint, *Doe v. Netflix, Inc.*, (N.D. Cal.

Pinning privacy hopes on the disclosure tort is problematic also because of the tort's dubious constitutional standing.<sup>66</sup> The Supreme Court has allowed liability for the dissemination of truthful information in only a limited number of circumstances.<sup>67</sup> Erwin Chemerinsky notes that in the areas of national security<sup>68</sup> and the protection of publicity<sup>69</sup> the Court has allowed some liability.<sup>70</sup> However, these exceptions are extremely rare:

[T]he reality is that there are very few cases in American history where the Supreme Court in any context has allowed liability for truthful speech. The First Amendment is based on the strong premise that knowledge is better than ignorance, and liability for truthful speech is inconsistent with that axiom.<sup>71</sup>

Thus far, the Court has avoided ruling directly on whether the tort is in fatal conflict with the First Amendment right to free speech.<sup>72</sup> “Liability for public disclosure of private facts should thus be limited to situations in which publication will endanger public safety.”<sup>73</sup>

In essence, the tort of public disclosure of private facts creates a tort for “truthful defamation.”<sup>74</sup> This is problematic because unlike defamation, which allows for truth as a defense, the public disclosure tort makes a person liable precisely because the information is true. This lack of a truth defense has been struck down previously by the Supreme Court in the area of criminal libel.<sup>75</sup> Concerns about the tort's constitutionality have lead the Supreme Court of North Carolina to refuse to adopt it in

---

Dec. 17, 2009) (C09-05903), 2009 WL 6305245. The case arose when Netflix released seemingly anonymous data about customer video rentals. The company released the data as part of a contest, which asked contestants to try to design a system that would recommend movies to subscribers based on the movies they had already watched and ranked. *See Netflix Prize*, NETFLIX, <http://www.netflixprize.com> (last visited July 4, 2011). Netflix was hoping that the contestants could improve upon the company's own “Cinematch” system. *Id.* There were “51,051 contestants on 41,305 teams from 186 different countries . . . participating in the contest and . . . Netflix had received 44,014 valid submissions from 5,169 different teams.” Complaint, *Doe v. Netflix, Inc.*, 2009 WL 6305245. Researchers were able to use the data supplied by Netflix along with publicly available information to attach names to movie rental histories. *Id.* In some cases, this information could be used to “out” gay movie renters. *Id.* Along with several California and federal statutory claims, the plaintiffs alleged a tortious public disclosure of private facts. *Id.* A second incarnation of the contest was canceled because of privacy concerns. Steve Lohr, *Netflix Cancels Contest After Concerns Are Raised About Privacy*, N.Y. TIMES, Mar. 13, 2010, at B3.

66. *See* Chemerinsky, *supra* note 32, at 424–26.

67. *Id.*

68. *See* *Near v. Minnesota*, 283 U.S. 697 (1931).

69. *See* *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562 (1977).

70. *See* *Braun v. Soldier of Fortune Magazine, Inc.*, 968 F.2d 1110, 1122 (11th Cir. 1992) (allowing liability for advertising illegal activity, in this case an advertisement for a contract killer).

71. Chemerinsky, *supra* note 32, at 425.

72. *See generally* *Florida Star v. B.J.F.*, 491 U.S. 524 (1989); *Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1975).

73. Chemerinsky, *supra* note 32, at 434.

74. *Doe v. Methodist Hosp.*, 690 N.E.2d 681, 687 (Ind. 1997).

75. *See* *Garrison v. Louisiana*, 379 U.S. 64, 71–73 (1964).

that state,<sup>76</sup> and several other states have refused to recognize it as a legal cause of action.<sup>77</sup> Even the Restatement (Second) of Torts includes a note highlighting public disclosure's constitutionally dubious nature.<sup>78</sup>

These problems make it unlikely that the disclosure tort will be of much use to those hoping to contain the use of private information. The requirement that the information be private, that its disclosure be highly offensive, that there be "publicity," and the First Amendment issues all show that there is little likelihood that this tort can be successfully used against data traders.

### C. APPROPRIATION

The tort of appropriation holds the best hope for those who want to use a traditional privacy tort to hold data collectors liable. On its face, appropriation seems to provide a cause of action for the use of private information. The Restatement (Second) of Torts assigns liability for appropriation to "[o]ne who appropriates to his own use or benefit the name or likeness of another."<sup>79</sup> The tort is often broken into three elements: (1) an appropriation, (2) without consent, (3) "of one's name or likeness for another's use or benefit."<sup>80</sup> The most common way that a person's likeness is appropriated is through the use of their name or image to advertise a product or business "or for some other commercial purpose."<sup>81</sup> The tort is not limited at common law to commercial uses, although some states so restrict it by statute.<sup>82</sup> For there to be liability, the defendant must "have appropriated to his own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness."<sup>83</sup> The tort "does not protect one's name per se; rather, it protects the value associated with that name."<sup>84</sup>

There are two reasons that the appropriation tort might appear to be the best tactic in creating liability for those who use and sell personal information.<sup>85</sup> The first is that it seems to create liability for mental distress and damages to the value of a person's identity.<sup>86</sup> Second is the

---

76. *Hall v. Post*, 372 S.E.2d 711, 714 (N.C. 1988).

77. See *Methodist*, 690 N.E.2d at 693; *Stubbs v. N. Mem'l Med. Ctr.*, 448 N.W.2d 78, 81 (Minn. Ct. App. 1989); *Hall*, 372 S.E.2d at 714.

78. RESTATEMENT (SECOND) OF TORTS § 652D special note (1977).

79. *Id.* § 652C.

80. *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1355 (Ill. App. Ct. 1995) (quoting RESTATEMENT (SECOND) OF TORTS § 652C (1977)).

81. RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1977).

82. *Id.*

83. *Id.* at § 652C cmt. c.

84. *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1009 (N.H. 2003).

85. *Ludington*, *supra* note 30, at 169.

86. *Id.*

breadth with which courts have defined “identity.”<sup>87</sup> “Data traders deal quite specifically in information that identifies a person, and the value of the information is based on the accuracy and completeness with which the person is identified.”<sup>88</sup> Because aggregation of information allows for the identification of the person, it could be argued that combining identifying information is enough to satisfy the tort.<sup>89</sup>

However, courts have been extremely reluctant to allow the appropriation tort to be used against data collectors and sellers.<sup>90</sup> In *Shibley*,<sup>91</sup> magazine publishers were sued for selling customer lists.<sup>92</sup> The Court of Appeals of Ohio held that this was not appropriation because the tort is meant to prevent situations where the plaintiff’s “name or likeness is displayed to the public to indicate that the plaintiff indorses the defendant’s product or business.”<sup>93</sup> Because the companies’ activities did not involve this kind of behavior, the appropriation tort was held to be inapplicable.<sup>94</sup>

The court in *Remsburg v. Docusearch, Inc.* used a different justification for not applying the appropriation tort to the sale of personal information.<sup>95</sup> In *Remsburg*, an Internet-based investigation service was sued after it sold information to a woman’s stalker.<sup>96</sup> Using the information supplied by Docusearch, the stalker was able to shoot and kill the woman outside her workplace.<sup>97</sup> The administratrix of the woman’s estate sued, arguing that the company was liable for appropriation after it sold the information to the stalker.<sup>98</sup> The Supreme Court of New Hampshire held that there was no liability for appropriation of likeness because the information’s value did not stem from the woman’s reputation or prestige. Instead, the information was independently valuable.<sup>99</sup>

---

87. *Id.*

88. *Id.*

89. *Id.*

90. See *Nelson v. Harrah’s Entm’t Inc.*, 2008 U.S. Dist. LEXIS 46524, at \*3–4 (N.D. Ill. June 13, 2008); *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1353 (Ill. App. Ct. 1995); *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1010 (N.H. 2003) (“An investigator who sells personal information sells the information for the value of the information itself, not to take advantage of the person’s reputation or prestige.”).

91. 341 N.E.2d 337 (Ohio Ct. App. 1975).

92. *Id.* at 338.

93. *Id.* at 339 (citing WILLIAM PROSSER, LAW OF TORTS § 117 (4th ed. 1971)).

94. *Id.* at 340.

95. 816 A.2d at 1005–06.

96. *Id.*

97. *Id.*

98. *Id.* at 1009.

99. *Id.* at 1010.

The investigator does not capitalize upon the goodwill value associated with the information but rather upon the client's willingness to pay for the information. In other words, the benefit derived from the sale in no way relates to the social or commercial standing of the person whose information is sold.<sup>100</sup>

Because of this distinction in value, the court held there was no cause of action against a person who sells the personal information of another.<sup>101</sup>

The holding in *Remsburg* is similar to that in *Dwyer*,<sup>102</sup> in which American Express cardholders sued the company for selling their purchasing information to third parties.<sup>103</sup> The Appellate Court of Illinois held that there was little or no value in an individual's name: "[A] single, random cardholder's name has little or no intrinsic value to defendants."<sup>104</sup> Instead, the information's value came from the defendants' "categorizing and aggregating" of the plaintiffs' names.<sup>105</sup> And the defendants' actions did not "deprive any of the cardholders of any value their individual names may possess."<sup>106</sup> Therefore, the plaintiffs failed to properly allege a tortious misappropriation.<sup>107</sup>

As Sarah Ludington notes, no data trader has ever been found liable for misappropriation,<sup>108</sup> and with the restraints courts have put on the tort, it seems unlikely that one ever will be. The tort of misappropriation is simply not a good fit for data collection, use, and sale. As the

---

100. *Id.*

101. *Id.* But see Ludington, *supra* note 30, at 170–71 (arguing that dicta in *Remsburg* could allow a suit to be brought when the data is sold for the value of the individual's "social or commercial standing"—their spending habits, preferences, interests, or creditworthiness").

102. *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995); see *supra* Part I.A for discussion of this case in relation to the intrusion tort.

103. *Dwyer*, 652 N.E.2d at 1353.

104. *Id.* at 1356.

105. *Id.*

106. *Id.*

107. See *In re Trans Union Corp. Privacy Litig.*, 326 F. Supp. 2d 893, 903 (N.D. Ill. 2004) (citing *Dwyer* positively and holding that plaintiffs must allege that "a specific reputation, prestige or social standing" was appropriated by the defendant). For an example of a court willing to use a broader definition of appropriation, see *Weld v. CVS Pharmacy, Inc.*, No. CIV. A. 98-0897F, 1999 WL 494114, at \*8 (Mass. Super. Ct. June 29, 1999); Ludington, *supra* note 30, at 171. In *Weld*, a pharmacy compiled a list of persons who were filling prescriptions for medication for certain illnesses. *Weld*, 1999 WL 494114, at \*1. It sold that list to pharmaceutical companies, which then sent out brochures. *Id.* The Massachusetts Superior Court denied the defendant's motion for summary judgment and held that commercial use of the information was not needed because appropriation "also applies when the defendant makes use of the plaintiff's name or likeness for his own purposes and benefit, even though the use is not a commercial one, and even though the benefit sought to be obtained is not a pecuniary one." *Id.* at \*6 (quoting RESTATEMENT (SECOND) OF TORTS 652B cmt. B (1977)). However, after the trial concluded, the court reexamined the case and held that there was no appropriation. *Kelley v. CVS Pharmacy, Inc.*, No. 98-0897-BLS2, 2007 WL 2781163, at \*6 (Mass. Super. Ct. Aug. 24, 2007). In that second case, the same court held that the state statute controlling appropriation allowed claims only when the defendant seeks to "take advantage" of the plaintiff's "reputation, prestige, or other value associated with him, for purposes of publicity." *Id.* at \*6 (quoting MASS. GEN. LAWS ANN. ch. 214, § 3A).

108. Ludington, *supra* note 30, at 171.

illustrations that accompany the Restatement (Second) of Torts indicate, appropriation was designed for a different sort of harm. It was designed to protect a person's image and name in public advertising, and has proven to be ill-suited to the field of data aggregation.<sup>109</sup>

All of the privacy torts suffer from the same problem with their design: they were conceived to prevent the harms of another era. Even if these individual problems could be fixed, the common law privacy regime, as it has been developed in the United States, likely would not be of much use in preventing the collection of small bits of information that are combined into something more intrusive than any of its parts.<sup>110</sup>

By its nature, tort law looks to isolated acts, to particular infringements and wrongs. The problem with databases does not stem from any specific act, but is a systemic issue of power caused by the aggregation of relatively small actions, each of which when viewed in isolation would appear quite innocuous.<sup>111</sup>

Unlike a naked picture in a magazine, a Peeping Tom, or a video used for commercial purposes, the individual bits of information collected from Internet users are unlikely to raise strong concerns. It is entirely possible that the person whose privacy has been "invaded" would never even know that an "intrusion" has taken place.<sup>112</sup> Thus, the traditional privacy torts are ill suited to solving the data collection problem.

## II. BREACH OF CONFIDENTIALITY

Because of the limitations of the traditional privacy torts, academics have attempted to expand the use of other torts to provide recovery for plaintiffs against data traders.<sup>113</sup> One of the more interesting is the notion of reviving the rarely used tort of breach of confidentiality.<sup>114</sup> Instead of protecting one's right to be "let alone," breach of confidentiality focuses on relationships rather than on the intrusion or the data itself.<sup>115</sup> While the United States was establishing its privacy common law around the ideas expressed by Warren and Brandeis<sup>116</sup> and codified by Prosser, the English were using confidentiality as a way to protect privacy rights.<sup>117</sup>

---

109. See RESTATEMENT (SECOND) OF TORTS § 652C cmt. a (1977).

110. See Solove, *supra* note 49, at 1434.

111. *Id.*

112. *Id.*

113. See G. Michael Harvey, Comment, *Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. PA. L. REV. 2385, 2425 (1992).

114. See, e.g., Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007); see also generally Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1 (1995); Stephanie D. Taylor, *Small Hope Floats?: How the Lower Courts Have Sunk the Right of Privacy*, 108 W. VA. L. REV. 459 (2005); Harvey, *supra* note 113; Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426 (1982).

115. Richards & Solove, *supra* note 114, at 125.

116. Ironically, Warren and Brandeis explicitly rejected using breach of confidence as a way to

A plaintiff can establish a breach by showing that there was a duty of confidentiality and then a breach of that duty.<sup>118</sup> “Courts have found the existence of such a duty by looking to the nature of the relationship between the parties, by reference to the law of fiduciaries, or by finding an implied contract of confidentiality.”<sup>119</sup> Most breaches of confidentiality have been found in cases against doctors, but courts have also applied it to banks, hospitals, insurance companies, psychiatrists, social workers, accountants, school officials, attorneys, and employees.<sup>120</sup> However, the most “clearly established” use of the tort involves physicians and banks.<sup>121</sup>

English courts hold that a duty of confidence can be created “by contract, the pre-existing relations of the parties, or the unilateral imposition of such a duty by the confider telling the confidant that the

---

protect privacy rights. Warren & Brandeis, *supra* note 20, at 210–11. They argued that betrayal of a confidence is too narrow to justify finding a breach: “[N]ow that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.” *Id.* at 211.

117. Richards & Solove, *supra* note 114, at 158–59; *see also* *Coco v. A.N. Clark (Eng’rs) Ltd.*, [1968] F.S.R. 415, 419 (Eng.). *Coco* held that there are three elements in a cause of action for breach of confidence: “First, the information itself . . . must have the necessary quality of confidence about it. Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it.” *Id.* (internal quotation marks and citations omitted). For a modern application of the law, *see* *A v. B plc.*, [2002] EWCA (Civ) 337, [2003] Q.B. 195, 195 (Eng.) (finding no breach of confidence in the publishing of details of a footballer’s affairs). *See generally* Basil Markesinis et al., *Concerns and Ideas About the Developing English Law of Privacy (And How Knowledge of Foreign Law Might Be of Help)*, 52 AM. J. COMP. L. 133 (2004) (summarizing the development of privacy law in England).

118. Richards & Solove, *supra* note 114, at 157.

119. *Id.*

120. *Id.* at 157–58 (citing *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 516 (4th Cir. 1999) (“The tort [of breach of duty of loyalty] applies when the employee breaches her employer’s confidences”)); *Ingram v. Mut. of Omaha Ins. Co.*, 170 F. Supp. 2d 907, 911 (W.D. Mo. 2001) (holding that an insurance company has a duty no different from that of a doctor or hospital to protect the private medical information it receives); *Peterson v. Idaho First Nat’l Bank*, 367 P.2d 284, 290 (Idaho 1961) (holding that the special relationship between a bank and its customer creates a duty to protect the customer’s confidential information); *Saur v. Probes*, 476 N.W.2d 496, 498 (Mich. Ct. App. 1991) (“[A] legal duty does exist on the part of a psychiatrist not to disclose privileged communications.”); *Rich v. N.Y. Cent. & Hudson River R.R. Co.*, 87 N.Y. 382, 390 (1882) (holding that a duty separate from a contractual obligation exists between a lawyer and his client); *Harley v. Druzba*, 169 A.D.2d 1001, 1002 (N.Y. App. Div. 1991) (“[T]he communications to be fostered in the social worker/client relationship are confidential and that plaintiff is entitled to invoke the privilege of professional confidence . . . .”); *Blair v. Union Free Sch. Dist. No. 6*, 324 N.Y.S.2d 222, 228 (N.Y. Dist. Ct. 1971) (holding that a school owes a duty of confidentiality to students and their families); *Biddle v. Warren Gen. Hosp.*, 715 N.E.2d 518, 523 (Ohio 1999) (holding that there is an independent tort for breach of confidence for the “unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship”); *Wagenheim v. Alexander Grant & Co.*, 482 N.E.2d 955, 961 (Ohio Ct. App. 1983) (holding that an accountant has a duty not to reveal private information about his clients);

121. Vickery, *supra* note 114, at 1428.

information is given in confidence.”<sup>122</sup> In some circumstances, English courts will impose a duty on a third party receiving the information as long as the party knows the information was given in confidence.<sup>123</sup> They also have applied the duty to a wide range of personal relationships, including spouses and close friends.<sup>124</sup> American courts, however, have limited the duty to close professional relationships, when they have found a duty at all.<sup>125</sup>

Breach of confidence in English law has its “roots in contract and fiduciary law” but is, in fact, a tort.<sup>126</sup> American courts have only recognized a cause of action under circumstances that have their roots in the law of contracts or fiduciary duties.<sup>127</sup> However, there has been a call for a separate tort of breach of confidence that would rid itself of the technical requirements of both contract law and fiduciary duties.<sup>128</sup> The way in which a court arrives at a breach of confidence cause of action matters, whether it be through contract law or through a fiduciary duty. Thus, this Note addresses each of these theories in turn.

#### A THE CONTRACT THEORY

There are two basic ways in which a duty of confidence can be established under a contract theory. The first is that of an express contract, in which one party agrees to divulge information on the condition that it remain secret. The most explicit of these agreements is not controversial.<sup>129</sup> Explicit contracts that limit the ability of the speaker

---

122. Gilles, *supra* note 114, at 10 (quoting *Marcel v. Comm’r of Police*, [1992] 1 All E.R. 72) (internal quotation marks omitted).

123. *Id.* at 12.

124. Gilles, *supra* note 114, at 13 n.64 (citing *Duchess of Argyll v. Duke of Argyll*, [1967] 1 Ch. 302, 329 (Eng.)) (“[The] policy of the law, so far from indicating that communication between husband and wife should be excluded from protection against breaches of confidence . . . strongly favours its inclusion.” (internal citation omitted)); see also *Stephens v. Avery*, [1988] 1 Ch. 449, 456 (Eng.) (holding that the duty of confidence extends to friends when the information is given to the friend on the condition that it remain confidential).

125. American courts have held third parties to a breach liable in some circumstances. See, e.g., *Hammonds v. Aetna Cas. & Sur. Co.*, 243 F. Supp. 793, 803 (N.D. Ohio 1965) (“[P]articipation in breaches of trust must also apply to one who participates in or induces the breach of any fiduciary duty.”).

126. Gilles, *supra* note 114, at 14.

127. *Id.* at 14–15.

128. A small number of jurisdictions recognize a separate, limited tort of breach of confidence. See, e.g., *Faris v. Enberg*, 158 Cal. Rptr. 704, 712 (Ct. App. 1979) (“An actionable breach of confidence will arise when an idea, whether or not protectable, is offered to another in confidence, and is voluntarily received by the offeree in confidence with the understanding that it is not to be disclosed to others, and is not to be used by the offeree for purposes beyond the limits of the confidence without the offeror’s permission.”); *Harley v. Druzba*, 169 A.D.2d 1001, 1002 (N.Y. App. Div. 1991) (holding that breach of confidence was a tort separate from a breach of contract cause of action). However, both New York and California “use contractual and fiduciary concepts to define the tort.” Gilles, *supra* note 114, at 53.

129. Gilles, *supra* note 114, at 15 (“Express written contracts, binding the signer to hold

are quite common in the area of employment.<sup>130</sup> The second way to establish a duty of confidence is through a sort of implied contract that is often close to fiduciary duty.<sup>131</sup> These implied contracts arise from the relationship between the contracting parties and are enforced “only when it is within the actual expectation of the parties.”<sup>132</sup> When the relationship involves “lawyers and other professional care-givers,” an implicit expectation of privacy comes with the contract for services.<sup>133</sup> However, the further the relationship gets from these special relationships, the less likely it is that confidentiality will be implied by the courts.<sup>134</sup>

There are two major problems with basing a breach of confidence claim on a contract theory. First, there is the issue of meeting the technical requirements of a contract claim.<sup>135</sup> There must be consideration,<sup>136</sup> which might be difficult to show in a situation where information is given to a company while surfing the Internet or making a purchase. The plaintiff might be required to show that she received something in return for the forfeiture of information. The plaintiff would also be required to show that the parties intended to make a contract.<sup>137</sup> Again, it would be difficult to show that the person who reveals information to a data collecting company intended to enter into a contract with that company. Second, the plaintiff might be required to show that the contract’s terms were “reasonably certain.”<sup>138</sup> If there is no written contract, it is difficult to show exactly what the person expected would happen with their information and what the legally binding obligations were for the data collecting company.<sup>139</sup>

But even if these technical problems can be solved, the problem of damages remains.<sup>140</sup> Contract law is ill-suited to recovery for damages associated with loss of reputation and mental distress.<sup>141</sup> Unfortunately for a plaintiff looking to sue a data-collecting company for using or selling her personal information, it is likely that these are her only real

---

information confidential, have long been used in the commercial area . . .”).

130. See 2 RUDOLPH CALLMANN, UNFAIR COMPETITION, TRADEMARKS AND MONOPOLIES § 14:6 (2010) (explaining that employment contracts can extend the obligation to protect information that might not otherwise be covered by trade secrets laws and can remain in effect after the employee leaves the job).

131. See *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 515 (4th Cir. 1999) (holding that the employment contract can create an implied duty of confidence).

132. Gilles, *supra* note 114, at 18.

133. *Id.* at 19.

134. *Id.*

135. *Id.* at 19–25.

136. RESTATEMENT (SECOND) OF CONTRACTS § 71 (1981).

137. See *id.* § 17.

138. *Id.* § 33.

139. The Statute of Frauds could also present a problem with unwritten contracts. See *id.* § 110.

140. Gilles, *supra* note 114, at 25–32.

141. *Id.* at 25–26.

damages. Also unavailable are punitive damages,<sup>142</sup> the only real remaining avenue for recovery.

One possible solution to the technical requirements of recovery under a contract theory is that of promissory estoppel.<sup>143</sup> This doctrine allows recovery even when the technical requirements of contract law are not met.<sup>144</sup> However, there still must have been a promise to keep the data private, and the person seeking recovery must show that she reasonably relied on that promise and changed her position as a result.<sup>145</sup> There is also the requirement that the court find that enforcing the promise will avoid “injustice.”<sup>146</sup>

These are all high hurdles for the typical plaintiff seeking recovery for the use and sale of her personal information. Showing a promise would be difficult, although possible, considering most companies that collect personal information maintain a privacy policy.<sup>147</sup> However, even if a plaintiff could show a promise, she would have to show that she relied on it and then, because promissory estoppel is an equitable remedy, the court would have to hold that enforcing the promise would prevent injustice. And even if all of these elements could be met, the plaintiff would still have the same problem with limited damages.

#### B. THE FIDUCIARY RELATIONSHIP THEORY

Instead of using contract law to establish a duty for the breach of confidence, some courts look to fiduciary duties to establish the requisite relationship. The Restatement (Second) of Torts provides that “[o]ne standing in a fiduciary relation with another is subject to liability to the other for harm resulting from a breach of duty imposed by the relation.”<sup>148</sup> A duty to keep private information confidential can be established using fiduciary duties.<sup>149</sup> This theory looks to the essence of the relationship, rather than to any agreement reached by the parties. Under traditional fiduciary law those in certain relationships are bound by the duty, including trustees, personal representatives of estates, guardians or conservators, partners in partnerships, joint venturers, agents and principals, co-owners, and attorneys.<sup>150</sup> But fiduciary

---

142. RESTATEMENT (SECOND) OF CONTRACTS § 355 (1981). *But see generally* William S. Dodge, *The Case for Punitive Damages in Contracts*, 48 DUKE L.J. 629 (1999).

143. *See* RESTATEMENT (SECOND) OF CONTRACTS § 90 (1981).

144. *Id.*

145. *See id.*

146. *Id.*

147. At least one state actually requires businesses that collect information from their customers on the Internet to have a privacy policy. *See* CAL. BUS. & PROF. CODE § 22575(a) (2010).

148. RESTATEMENT (SECOND) OF TORTS § 874 (1979).

149. *See* Gilles, *supra* note 114, at 39–40.

150. CARYL A. YZENBAARD ET AL., *THE LAW OF TRUSTS AND TRUSTEES* § 481 (3d ed. 2009).

relationships are not limited to those listed and can arise as the facts and circumstances demand.<sup>151</sup>

The law of confidentiality, however, is more expansive than the traditional fiduciary duties.<sup>152</sup>

A confidential relation exists between two persons when one has gained the confidence of the other and purports to act or advise with the other's interest in mind. A confidential relation may exist although there is no fiduciary relation; it is particularly likely to exist where there is a family relationship or one of friendship or such a relation of confidence as that which arises between physician and patient or priest and penitent.<sup>153</sup>

Sometimes the terms “fiduciary” and “confidential” will be used interchangeably.<sup>154</sup> But the term “confidential relation” is used “when the relationship is similar to those noted in a fiduciary relation but does not fit into one of the well-defined categories of fiduciary law.”<sup>155</sup> It is an equitable concept that lacks a concrete definition. However, cases in which confidential relationships have been found tend to emphasize “great intimacy, disclosure of secrets, entrustment of power, and superiority of position.”<sup>156</sup>

The relationship between the person giving up her information and the company collecting it simply does not meet the required criteria. There is no “great intimacy” nor is there any “entrustment of power.” The superiority of position is questionable when a consumer has many ways of buying a product or service, is simply ignorant of the privacy considerations, or doesn't really care whether the company collects information about her. Even the depth of the secrets divulged is questionable. Most of the personally identifying information is not terribly personal until it is combined with other information by companies that aggregate information. While medical records or detailed financial information might meet the secrecy requirement, a person's name, address, and list of hobbies likely will not.

151. *Id.*

Courts asked to find a fiduciary relationship in a new context will first identify a relationship that the law already recognizes as having fiduciary status. Using that relationship as a model for analyzing the relationship at issue, the courts will next evaluate whether the instant relationship is sufficiently like the model relationship to support recognizing it as fiduciary.

Marcey L. Grigsby, Book Review, *Seeking Privacy: Examining a Role for the Fiduciary in Protecting Personal Information*, 50 N.Y.L. SCH. L. REV. 1031, 1051–52 (2005) (reviewing DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* (2004)).

152. See RESTATEMENT (SECOND) OF TRUSTS § 2 cmt. b (1973).

153. *Id.*

154. YZENBAARD ET AL., *supra* note 150, § 482.

155. *Id.*

156. *Id.*; see also *Snepp v. United States*, 444 U.S. 507, 510–11 (1980) (per curiam) (holding that a former CIA employee breached an obligation to the CIA by publishing information he learned during his employment without first submitting the information to the agency).

Solove proposes that fiduciary relationships be expanded to include those businesses that hold personal information.<sup>157</sup> He bemoans the fact that the relationship between collectors and users of personal data “is akin to the relationship between strangers—with one very important difference: One of the strangers knows a lot about the other and often has the power to use this information to affect the other’s life.”<sup>158</sup> Solove concedes that his proposal is a “radical” one and admits that courts have thus far been unwilling to extend fiduciary duties so far.<sup>159</sup> He argues that fiduciary law is flexible enough to impose a duty on companies that hold personal information.<sup>160</sup>

However, expanding the duty of confidence to embrace more relationships has its drawbacks.<sup>161</sup> First, there is the issue of where to draw the line. It seems highly problematic to impose fiduciary duties in arms-length commercial transactions and web searches. It is well-established law that buyers and sellers have no fiduciary duties to each other.<sup>162</sup> Second, even if one party places “trust or confidence in the other,” an arms-length transaction does not create a fiduciary duty absent “some recognition, acceptance or undertaking of the duties of a fiduciary on the part of the other party.”<sup>163</sup> To say simply that anyone who possesses private information owes a duty of confidence to the person to whom the data relates, without some strong limiting principle, would create unending liability: “In our lives as social beings we are forced to rely on librarians, police officers, bank tellers, telephone operators and many more. Do every one of these relations qualify as confidential?”<sup>164</sup> And imposing a duty on those with whom a person conducts business in no way controls those who collect personal information outside of the buyer-seller relationship.

As with establishing a duty under contract law, establishing a duty of confidence under fiduciary law provides the plaintiff with limited damages.<sup>165</sup> Restitutionary damages are possible in the form of

---

157. SOLOVE, *supra* note 2, at 103.

158. *Id.* at 102.

159. *Id.* at 103.

160. *Id.* at 103–04.

161. See Gilles, *supra* note 114, at 46–48; see also Grigsby, *supra* note 151, at 1053–55.

162. *Nifty Foods Corp. v. Great Atl. & Pac. Tea Co.*, 614 F.2d 832, 838 (2d Cir. 1980) (“The relationship of a buyer to his supplier, even if that buyer accounts for the large part of the supplier’s business, does not constitute a fiduciary or other special relationship of trust . . .”), *superseded by statute as recognized in* *Rosenfeld v. Basquiat*, 78 F.3d 84 (2d Cir. 1996); see also *Alexander v. CIGNA Corp.*, 991 F. Supp. 427, 438 (D.N.J. 1998) (“[F]iduciary duties are not imposed in ordinary commercial business transactions.”); *Paul v. North*, 380 P.2d 421, 426 (Kan. 1963) (“[A fiduciary relationship exists in business transactions only] when, by their concerted action, they willingly and knowingly act for one another in a manner to impose mutual trust and confidence that a fiduciary relationship arises.”).

163. *Lanz v. Resolution Trust Corp.*, 764 F. Supp. 176, 179 (S.D. Fla. 1991).

164. Gilles, *supra* note 114, at 46–47.

165. See *id.* at 48–51.

“disgorgement of any monetary gain by the fiduciary or the imposition of a constructive trust.”<sup>166</sup> Damages are evaluated by looking at the gain to the defendant rather than at the loss to the plaintiff,<sup>167</sup> something that can be extremely difficult to measure. However, it is probable that, like a cause of action under contract law, the plaintiff will not be able to recover for emotional distress.<sup>168</sup> The recovery for any one plaintiff would probably be very little, because the measure of profit by the company in retaining and selling the information of one individual is likely to be small.<sup>169</sup>

### C. CREATING A TORT

At least two states, New York and California, have created a separate tort of breach of confidence, which exists outside of fiduciary duties and contract law. Both states, however, continue to rely on fiduciary duties and contract law to define the scope of the tort. California relies heavily on contract law to define the tort's scope and confines it to cases where the parties have knowledge that confidence is required.<sup>170</sup> This reliance on contract law likely springs from the fact that most breach of confidence cases in California concern “the revelation of an idea for a show or movie.”<sup>171</sup> New York, however, bases the scope of the tort on either fiduciary relationships or implied contract.<sup>172</sup>

The benefit of creating a tort separate from fiduciary duties and contract law is twofold. First, damages are not as restricted in a tort action as they are under a fiduciary or contract cause of action. Second, the technical requirements of both contract and fiduciary law can be largely ignored. However, one large practical problem that plagues both contractual and fiduciary causes of action remains, even if the cause of action is defined as one in tort law. Knowing which relationships are covered by the tort is difficult, as there will still be the need to attach liability in arms-length transactions. Simply defining the action as a tort still requires the court to decide if the relationship is one that should be covered by the tort, whether the relationship springs from a contract-like duty or is established without the need for the parties to agree that the information remain confidential.

---

166. *Id.* at 48.

167. Taylor, *supra* note 114, at 491.

168. See *Kohler v. Fletcher*, 442 N.W.2d 169, 172 (Minn. Ct. App. 1989); *Lash v. Cheshire Cnty. Sav. Bank, Inc.*, 474 A.2d 980, 982 (N.H. 1984) (*per curiam*); see also RESTATEMENT (SECOND) OF TRUSTS § 197 (1973) (“Except as stated in § 198, the remedies of the beneficiary against the trustee are exclusively equitable.”).

169. A class action lawsuit might solve this problem, but examination of this idea is beyond the scope of this Note.

170. See *Faris v. Enberg*, 158 Cal. Rptr. 704, 713 (Ct. App. 1979).

171. Gilles, *supra* note 114, at 54.

172. *Id.*

### III. INFORMATION AS A PROPERTY RIGHT

Another method for protecting against data trading would be to establish a property right in private information.<sup>173</sup> Scholars have proposed creating this right in response to the problems associated with trying to protect those privacy rights through torts.<sup>174</sup> This response is understandable, considering the limits that tort and contract law impose for those trying to keep personal information from being collected, sold, or stolen. But there is a fundamental flaw in the use of property rights to protect the private information of individuals.<sup>175</sup> At its core, granting a property right to information is essentially creating a property right in facts:

Our society has a longstanding commitment to freedom of expression. Property rights in any sort of information raise significant policy and free speech issues. Facts are basic building blocks: building blocks of expression; of self-government; and of knowledge itself. When we recognize property rights in facts, we endorse the idea that facts may be privately owned and that the owner of a fact is entitled to restrict the uses to which that fact may be put. That notion is radical.<sup>176</sup>

The Supreme Court has considered and rejected the notion that one can create a property right in facts and keep others from using those facts.<sup>177</sup> In *Harper & Row, Publishers, Inc. v. Nation Enterprises*, the Court held that copyright law is constitutional but included an important caveat: The First Amendment does not allow an author to copyright his ideas or facts.<sup>178</sup> “[A]ll facts—scientific, historical, biographical, and news of the

173. See, e.g., Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63 (1999); see also Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 383 (2003).

174. Bergelson, *supra* note 173, at 414. Bergelson argues there are three reasons that a property-based solution is superior to a tort-based solution: “(i) the torts approach cannot support a consistent, workable mechanism for the enforcement of information privacy rights; (ii) U.S. law, explicitly or implicitly, already regards personal information as property; and (iii) the property regime better serves the interests of individual parties and society in general.” *Id.*

175. Scholars have come up with other reasons to be skeptical of creating a property right in one’s own property. Those include a market-based argument, which argues that, rather than constrain data trading, creating a property right in personal facts will create a more robust market in private information than currently exists. See Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1295–96 (2000). These criticisms are beyond the scope of this Note.

176. *Id.* at 1294.

177. See Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1065–68 (2000).

178. 471 U.S. 539, 556 (1985). (“[C]opyright’s idea/expression dichotomy ‘strike[s] a definitional balance between the First Amendment and the Copyright Act by permitting free communication of facts while still protecting an author’s expression.’” (quoting *Harper & Row, Publishers, Inc. v. Nation Enters.*, 723 F.2d 195, 203 (2d Cir. 1983))). The idea that there is no property right in facts is not new. See *Int’l News Serv. v. Assoc. Press*, 248 U.S. 215, 246 (1918) (Holmes, J., dissenting) (“[T]here is no property in the combination or in the thoughts or facts that the words express. Property, a creation of law, does not arise from value, although exchangeable—a matter of fact.”); see also *U.S. News & World Report, Inc. v. Avrahami*, No. 95-1318, 1996 Va. Cir. LEXIS 518, at \*16 (Va. Cir. June 13, 1996) (holding that there is no property right in a name).

day . . . may not be copyrighted and are part of the public domain available to every person.”<sup>179</sup> Similarly, trademark law does not extend the right to exclude others from the use of opinions and facts, “even if the speech uses the product’s name.”<sup>180</sup>

The prohibition on creating a property right in facts is understandable. It is difficult to see how one would define what is covered by the property right. Is it the combining together of facts together that forms a right to privacy? Would the law have to create safe havens of fair use for noncommercial use of this private information? How would this property right be enforced when private information such as names, addresses, credit card numbers, and other financial and consumer information is required to conduct a vast amount of business both in person and on the Internet?

All of these questions point to the ultimate reason that property, tort, and contract law are the wrong solution to the problem. Counting on judge-made common law to regulate such a fast moving and invasive problem is simply inadequate. Even if courts could find a way to avoid the problems with privacy torts, breach of confidence, and property law, it would be a slow and inconsistent process that would allow the problem to fester for many years before a solution could be found. That is why this Note advocates a statutory or regulatory solution to the problem. State legislatures and Congress, either on its own or through power delegated to the FTC, have the ability to craft flexible, responsive solutions that carefully target the problem without creating First Amendment conflicts.

#### IV. THE CURRENT STATE OF STATUTORY AND REGULATORY LAW

The laws governing the use of private information in private commercial databases have been roundly criticized. The statutory and regulatory scheme has been called inconsistent, unpredictable, and haphazard.<sup>181</sup> But the latest indications are that states and the federal government have begun to take concerns over databases of personal information seriously. David Vladeck, the head of the Bureau of Consumer Protection at the FTC, said his agency is planning on getting tougher with companies that collect personal information from customers on the Internet,<sup>182</sup> and the FTC has proposed a so-called “No

---

179. *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 348 (1991) (internal quotation marks omitted).

180. Volokh, *supra* note 177, at 1067. The other main area of intellectual property is patent law, but its application to this problem is inappropriate as patent law deals with inventions and processes, not pieces of information. See 35 U.S.C. § 101 (2006).

181. Ludington, *supra* note 30, at 151.

182. Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 5, 2009, at B1; see also Thomas Claburn, *FTC Examining Cloud Computing*, INFORMATIONWEEK (Jan. 5, 2010), <http://www.informationweek.com/news/government/policy/222200380>; John Letzing, *FTC Has*

Track List” to protect Internet users.<sup>183</sup> And, at least when it comes to protecting consumers from identity theft, there has been a lot of action on the part of both state and local government in recent years.

#### A. FEDERAL LAW

Congress has passed several laws that directly affect those who collect and use private information. The vast majority of these laws can be divided into two categories. First, there are privacy laws that cover financial institutions. These laws cover everything from the right to inspect records to the ability to share information. The second category is more of a mishmash. These laws target specific kinds of information deemed to be so private as to deserve special protection. Congress has stepped in to create statutory protection for medical information and media consumption habits. Some of these laws create severe restrictions on any dissemination, some try to create protection for victims of identity theft, and still others limit the ability to collect the information in the first place.

##### 1. *Financial Information*

With the dawn of the computer age came attempts by Congress to address the privacy concerns revolving around the large amount of financial information beginning to accumulate in private databases.<sup>184</sup> In 1970, Congress passed the Fair Credit Reporting Act (FCRA),<sup>185</sup> which attempted to ensure “[a]ccuracy and fairness” in the credit-reporting system by giving people the right to inspect their credit records and correct any mistakes in them, as well as limiting the use and disclosure of information to third parties.<sup>186</sup>

Decades later, Congress passed the Gramm-Leach-Bliley Act.<sup>187</sup> This Act places significant restrictions on the ability of financial institutions<sup>188</sup> to share their customers’ nonpublic personal information<sup>189</sup>

---

*“Particular Interest” in Facebook Privacy*, MARKETWATCH (Jan. 19, 2010), <http://www.marketwatch.com/story/ftc-has-particular-interest-in-facebook-privacy-2010-01-19>.

183. See *infra* Part V.E.1.

184. See CHRISTOPHER WOLF, PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 2:1.1 (1st ed. 2007).

185. 15 U.S.C. §§ 1681–1681u (2006).

186. *Id.* However, FRCA’s reach is limited to “consumer reporting agenc[ies].” 15 U.S.C. § 1681a(f) (2006). The definition of a consumer reporting agency extends beyond the three major reporting agencies—Equifax, Experian, and Trans Union—but is still limited by the definition contained in FRCA. See WOLF, *supra* note 184, § 2:2.2[C].

187. 15 U.S.C. §§ 6801–6809 (2006). Gramm-Leach-Bliley is also known as the Financial Services Modernization Act of 1999. BROWNLEE & WALESKI, *supra* note 188, § 1.05[4], at 1–59.

188. A “financial institution” is defined as “any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12.” *Id.* § 6809(3)(A). See CHARLENE BROWNLEE & BLAZE D. WALESKI, PRIVACY LAW § 3.03[1] (2010) for a full description of the wide range of businesses covered by the law. The complex and broad language of the statute means that many

with “nonaffiliated third part[ies].”<sup>190</sup> It requires financial institutions who wish to share their customers’ nonpublic personal information to notify their customers once a year about what information is collected and how it is used.<sup>191</sup> It also requires that the customer have the ability to opt out.<sup>192</sup>

Congress has also responded in recent years to the threats posed by identity theft. In 2003, Congress amended the FCRA by passing the Fair and Accurate Credit Transactions Act.<sup>193</sup> This Act gives victims of identity theft the ability to put an alert on their credit report<sup>194</sup> and block information resulting from identity theft.<sup>195</sup> It now also requires that merchants truncate debit and credit card numbers and remove expiration dates on sales slips.<sup>196</sup>

## 2. *Information-Specific Statutes*

In addition to laws that protect financial information, Congress has passed a series of laws that protect specific kinds of information. The Video Privacy Protection Act<sup>197</sup> is a statute that bans a “video tape service provider” from knowingly providing “identifiable information” about a customer to anyone.<sup>198</sup> The statute essentially bans movie rental and sales companies from sharing a customer’s rental or sales information. The Health Insurance Portability and Accountability Act includes provisions forbidding the dissemination of health care

---

institutions that do not consider themselves financial institutions might be covered by the Act. *See* KENNEDY, *supra* note 5, § 3.1.1, at 57. “Some travel agencies, for example, appear to be within the definition, as are retailers that offer their own installment payment accounts.” *Id.*

189. Nonpublic personal information “means personally identifiable financial information—(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. 15 U.S.C. § 6809(4)(A).

190. *Id.* § 6802(a).

191. KENNEDY, *supra* note 5, § 3.1.2.

192. *Id.* Gramm-Leach-Bliley creates a complex web of regulation, tasking members of eight different agencies with implementing regulations: the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, the Board of the National Credit Union Administration, the Securities and Exchange Commission, and the FTC. *Id.* § 3.1.1. In addition to the federal agencies tasked with enforcement of the Act, state insurance regulators govern those “engaged in providing insurance.” *Id.* However, the differences in regulations of the agencies only varies slightly. *Id.*; *see also* Kathleen A. Hardee, *The Gramm-Leach-Bliley Act: Five Years After Implementation, Does the Emperor Wear Clothes?*, 39 CREIGHTON L. REV. 915, 936–37 (2006) (suggesting that the Act’s accomplishments have been limited).

193. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 111 Stat. 1952 (codified as amended in scattered sections of 5, 10, 15, and 31 U.S.C.).

194. 15 U.S.C. § 1681c-1 (2006).

195. *Id.* § 1681c-2.

196. *Id.* § 1681c(g).

197. 18 U.S.C. § 2710 (2006).

198. *Id.* § 2710(b)(1).

information.<sup>199</sup> Congress also has restricted the use and disclosure of Social Security numbers<sup>200</sup> and the dissemination of school records.<sup>201</sup> The Cable Communications Policy Act<sup>202</sup> protects cable subscriber information by requiring cable companies to give notice of what information they are collecting and how it is being used.<sup>203</sup> This Act also prohibits cable companies from collecting personally identifiable information using the cable system or disclosing such information without the prior consent of the customer.<sup>204</sup> Similarly, the Telecommunications Act protects against the disclosure of individually identifiable subscriber data by a telecommunications carrier without prior approval.<sup>205</sup>

### 3. *Other Federal Laws*

Congress has not limited itself to the protection of particular kinds of information or information being held by particular kinds of organizations. For instance, the Computer Fraud and Abuse Act of 1996 prohibits unauthorized access to a computer to access protected data.<sup>206</sup> The Sarbanes-Oxley Act, while chiefly known for reforming corporate governance, requires public companies to maintain adequate “internal controls” on information.<sup>207</sup> This language has been construed to cover the protection of private information held by the companies. “Presumably, ‘internal controls’ cannot be achieved without adequate data protection mechanisms for financial information.”<sup>208</sup>

Congress has also moved to protect at least one particular class of individuals from data collection. The Children’s Online Privacy Protection Act provides special protection for those under the age of thirteen.<sup>209</sup> The Act requires that any commercial website that is directed at children under the age of thirteen get verifiable parental consent

---

199. See Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); 45 C.F.R. § 164.502 (2009).

200. 42 U.S.C. § 405(c)(2)(C)(viii) (2006).

201. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) (2006). This Act does not allow for a private right of action, but at least one court has implied a private right of action. *Fay v. S. Colonie Cent. Sch. Dist.*, 802 F.2d 21, 33–34 (2d Cir. 1986).

202. 47 U.S.C. § 551 (2006).

203. *Id.* § 551(a)(1).

204. *Id.* § 551(b)–(c). The restrictions on cable providers do not extend to instances in which cable companies provide Internet service. See *Klimas v. Comcast Cable Commc’ns, Inc.*, 465 F.3d 271, 279–80 (6th Cir. 2006); see also *AT&T Corp. v. City of Portland*, 216 F.3d 871, 876–77 (9th Cir. 2000).

205. 47 U.S.C. § 222(c)(1) (2006). The Telecommunications Act does not apply to Internet service. See *BROWNLEE & WALESKI, supra* note 188, § 1:05[6] at 1–61.

206. 18 U.S.C. § 1030 (2006). The definition of protected data is broad and includes information on any “protected computer.” *Id.* § 1030(a)(2)(C). A “protected computer” is defined as any computer that “is used in or affecting interstate or foreign commerce or communication.” *Id.* § 1030(e)(2)(B).

207. 15 U.S.C. § 7262 (2006).

208. *WOLF, supra* note 184, § 2:8, at 2–82.

209. 15 U.S.C. §§ 6501–6506 (2006).

before it can collect, use, or disclose personal private information about the children.<sup>210</sup>

These laws do a decent job of identifying the kinds of information that need the most protection, but they do not go far enough. Major categories of information that deserve protection have not been addressed. Federal law has simply not kept up with the realities of twenty-first century technological innovation. More must be done to protect online activities from prying eyes and to prevent information theft before it happens. And the federal government is in the best position to do more. Unlike the states, Congress has the ability to create uniform laws that will allow both businesses and consumers to be more certain where they stand.

#### B. ADMINISTRATIVE LAW

Congress has delegated authority to the FTC to stop unfair or deceptive acts or practices. With that authority, the FTC requires the proper disposal of private information,<sup>211</sup> and under the Red Flags Rule, the FTC has sought to prevent identity theft through more strict control over how personal information is kept.<sup>212</sup> The FTC also launches enforcement actions against companies that it deems to have engaged in deceptive acts or practices.<sup>213</sup>

The FTC, along with several other federal agencies, issued the Red Flags Rule in late 2007.<sup>214</sup> The rule requires all financial institutions and creditors to implement programs designed to detect, prevent, and mitigate identity theft in “covered accounts.”<sup>215</sup> “Financial institutions” are defined by reference to the Fair Credit Reporting Act<sup>216</sup> and include savings and loan associations, banks, and credit unions.<sup>217</sup> “Creditors” are

---

210. *Id.*

211. 16 C.F.R. § 682.3 (2010).

212. *Id.* § 681.1.

213. See *In re Sears Holdings Mgmt. Corp.*, F.T.C. File No. 0823099 (Aug. 31, 2009) (holding Sears responsible for collecting too much information about customers who volunteered to have some information collected from them as they surfed the Internet); *Sears Settles FTC Charges Regarding Tracking Software*, FTC (Jun. 4, 2009), <http://www.ftc.gov/opa/2009/06/sears.shtm>.

214. 12 C.F.R. § 222.90 (2010); 16 C.F.R. § 681.2 (2010).

215. A covered account is defined as:

- (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account;
- and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

12 C.F.R. § 222.90(b)(3).

216. *Id.* § 222.90(b)(7); see also 15 U.S.C. § 1681a(t) (2006).

217. 15 U.S.C. § 1681a(t).

defined more broadly and include “lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.”<sup>218</sup>

The Red Flags Rule adopts a flexible structure for businesses to design their own theft-prevention programs.<sup>219</sup> The rule simply requires each covered institution to implement a program designed to prevent identity theft.<sup>220</sup> It provides some guidelines,<sup>221</sup> but essentially the rule requires only that the program be “appropriate to the size and complexity of the [institution] and the nature and scope of its activities.”<sup>222</sup>

The Red Flags Rule is a good start, but still leaves far too many companies out. The rule applies only to financial and credit-giving companies, leaving many customers outside its protection. And it remains to be seen whether increasing the FTC’s regulatory power will be a good thing. The high-tech industry is worried that increased authority would give the FTC too much power to levy massive fines on those who are merely “aiding and abetting” those found in violation of the rule.<sup>223</sup>

### C. STATE LAWS

While the federal government has been somewhat cautious, in many cases states have passed much more expansive and robust laws. States have acted most aggressively in the attempt to prevent data theft and identity theft. But states have not stopped there; many states, led by California, have adopted statutes that govern the collection, use, and sale of personal information.

#### I. Notification Laws

One of the most widely adopted state efforts in the regulation of databases is mandatory notification in the event of a data-security breach.<sup>224</sup> California was the first state to pass such a law, and more than

218. 12 C.F.R. § 222.90(b)(5). “The term ‘creditor’ means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.” 15 U.S.C. § 1691(a)(e) (2006).

219. See 12 C.F.R. § 222.90(c)–(f) (2010).

220. See *id.*

221. See *id.* § 222.90(d)(2).

222. *Id.* § 222.90(d)(1).

223. Mike Shields, *Patrolling Bad Behavior*, MEDIAWEEK, Mar. 22, 2010, at 4.

224. CAL. CIV. CODE § 1798.82 (2010); see also ARIZ. REV. STAT. § 44-7501 (2011); ARK. CODE ANN. § 4-110-105 (2011); COLO. REV. STAT. § 6-1-716 (2011); CONN. GEN. STAT. § 36a-701b (2011); DEL. CODE tit. 6, § 12B-102 (2011); D.C. CODE § 28-3852 (2011); FLA. STAT. § 817.5681 (2011); GA. CODE ANN. § 10-1-912 (2011); HAW. REV. STAT. § 487N-2 (2008); IDAHO CODE ANN. § 28-105 (2004); 815 ILL. COMP. STAT. ANN. § 530/10 (West 2008); IND. CODE § 24-4.9-3-1 (2011); IOWA CODE ANN. § 715C.2 (West Supp. 2011); KAN. STAT. § 50-7a02 (2011); LA. REV. STAT. § 51:3074 (2011); ME. REV. STAT. tit. 10,

forty states have followed California's lead and passed their own statutes. California's law provides that state residents must be given notice if there is a security breach of unencrypted computer records that exposes their private information.<sup>225</sup>

While these laws have proven useful in some instances, they contain many loopholes. For example, most notification statutes require that notice be given only in the event that unencrypted computer records are stolen. Of the forty-four states that have these laws, only nine require notification if encrypted data is stolen.<sup>226</sup> And only two states require notification any time there is a breach of personal data, regardless of the format in which it is kept.<sup>227</sup> There are other ways companies can avoid the notification requirements. Connecticut allows companies to avoid notification if, after "investigation and consultation with . . . law enforcement" the company "reasonably determines that the breach will not likely result in harm."<sup>228</sup> Many states require notification only if the

§ 1348 (Supp. 2010); MD. CODE ANN., COM. LAW § 14-3504 (LexisNexis 2011); MASS. GEN. LAWS ch. 93H, § 3 (West 2008); MICH. COMP. LAWS § 445.72 (2011); MINN. STAT. ANN. § 325E.61 (West Supp. 2010); MONT. CODE ANN. § 30-14-1704 (2010); NEB. REV. STAT. § 87-803 (2011); NEV. REV. STAT. § 603A.220 (2009); N.H. REV. STAT. ANN. § 359-C:20 (LexisNexis 2008); N.J. STAT. ANN. § 56:8-163 (West Supp. 2011); N.Y. GEN. BUS. LAW § 899-aa (2011); N.C. GEN. STAT. ANN. § 75-65 (West Supp. 2010); N.D. CENT. CODE § 51-30-02 (2007); OHIO REV. CODE ANN. § 1349.19 (LexisNexis Supp. 2011); OKLA. STAT. tit. 74, § 3113.1 (2011); OR. REV. STAT. § 646A.604 (2009); 73 PA. CONS. STAT. ANN. § 2303 (West 2008); R.I. GEN. LAWS § 11-49.2-3 (Supp. 2010); TENN. CODE ANN. § 47-18-2107 (2011); TEX. BUS. & COM. CODE § 521.053 (2010); UTAH CODE § 13-44-202 (West 2011); VT. STAT. ANN. tit. 9, § 2435 (2011); VA. CODE § 18.2-186.6 (2011); WASH. REV. CODE § 19.255.010 (2011); W. VA. CODE ANN. § 46A-2A-102 (LexisNexis Supp. 2011); WIS. STAT. § 134.98 (2010); WYO. STAT. ANN. § 40-12-502 (2011); S.B. 453, 117th Gen. Assemb., Reg. Sess. (S.C. 2008).

225. CAL. CIV. CODE § 1798.82 (2010). "Personal information" has a detailed definition under the California law. It is the person's name in combination with her Social Security number, driver's license number, information that would permit access to a person's financial accounts, medical information, or health insurance information. *Id.* § 1798.82(e). Other states have more expansive definitions of what is personal information. North Carolina has a particularly detailed definition. *See* N.C. GEN. STAT. ANN. § 14-113.20 (West Supp. 2010) ("'[I]dentifying information' as used in this [Note] includes the following: (1) Social security or employer taxpayer identification numbers. (2) Drivers license, State identification card, or passport numbers. (3) Checking account numbers. (4) Savings account numbers. (5) Credit card numbers. (6) Debit card numbers. (7) Personal Identification (PIN) Code . . . . (8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names. (9) Digital signatures. (10) Any other numbers or information that can be used to access a person's financial resources. (11) Biometric data. (12) Fingerprints. (13) Passwords. (14) Parent's legal surname prior to marriage."); *see also id.* §§ 75-61(10), 75-65(a).

226. ALASKA STAT. § 45.48.090(7) (2010); IND. CODE § 24-4.9-3-1(a)(2) (2011); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(1)(b); N.Y. GEN. BUS. LAW § 899-aa(b); N.C. GEN. STAT. ANN. § 75-61(14) (West Supp. 2010); 73 PA. CONS. STAT. ANN. § 2303(b); VA. CODE § 18.2-186.6(c); W. VA. CODE ANN. § 46A-2A-102(b).

227. IND. CODE § 24-4.9-2-2 (2011) (protecting "computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format"); N.C. GEN. STAT. § 75-61(12) (2008) (requiring notice of breach of data whether it is "written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics").

228. CONN. GEN. STAT. § 36a-701b(b) (2011).

personal information is actually compromised.<sup>229</sup> This is in contrast to other states that require “acquisition” of data before the notification requirement is triggered.<sup>230</sup> This distinction makes such acquisition laws “appear more stringent.”<sup>231</sup> Some states also require that the breach materially compromise security before notification requirements become effective.<sup>232</sup>

California and Utah each have an additional notification law. These states require that businesses notify their customers when they intend to disclose information about them to a third party for direct marketing purposes or for compensation.<sup>233</sup> California also requires credit card issuers to allow their customers to opt out of disclosures to third parties.<sup>234</sup>

## 2. *Disposal and Minimum Security Statutes*

In a further effort to prevent security theft, many states require the secure disposal of private records.<sup>235</sup> Kentucky’s statute is a typical example of these laws, which seek to prevent identity theft by making sure that no private information falls into the wrong hands after it is thrown away.<sup>236</sup> “When a business disposes of . . . any customer’s records . . . the business shall take reasonable steps to destroy . . . that portion of the records containing personally identifiable information by shredding, erasing, or otherwise modifying [the information] to make it unreadable.”<sup>237</sup>

A few states have gone even further to keep private information from falling into the wrong hands. Several states now require a minimum level of security anytime they hold personal information, whether it is being disposed of or not.<sup>238</sup> These statutes are written in broad terms and

229. WOLF, *supra* note 184, § 2:9.3[C], at 2-85; *see, e.g.*, CAL. CIV. CODE § 1798.82(d).

230. WOLF, *supra* note 184, § 2:9.3[C], at 2-87 to 2-88; *see, e.g.*, CONN. GEN. STAT. § 36a-701b(a).

231. WOLF, *supra* note 184, § 2:9.3[C], at 2-88.

232. *See, e.g.*, FLA. STAT. § 817.5681(4) (2011).

233. CAL. CIV. CODE § 1798.83 (2010); UTAH CODE § 13-37-201.

234. CAL. CIV. CODE §§ 1748.10–1748.12.

235. ARIZ. REV. STAT. § 44-7601 (2011); ARK. CODE ANN. § 4-110-104(a) (2011); CAL. CIV. CODE § 1798.81; COLO. REV. STAT. § 6-1-713 (2011); GA. CODE ANN. § 10-15-2 (2011); 720 ILL. COMP. STAT. ANN. § 5/16G-21 (West Supp. 2011); IND. CODE § 24-4-14-1 (2011); KY. REV. STAT. ANN. § 365.725 (West 2006); MD. CODE ANN., COM. LAW §§ 14-3501–06 (LexisNexis 2011); MICH. COMP. LAWS § 445.72 (2011); MINN. STAT. ANN. § 325E.61 (West Supp. 2010); MONT. CODE ANN. § 30-14-1703 (2010); NEV. REV. STAT. § 603A.200 (2009); N.J. STAT. ANN. § 56:8-162 (West Supp. 2011); N.Y. GEN. BUS. LAW § 399-h (2011); N.C. GEN. STAT. ANN. § 75.64 (West Supp. 2010); TENN. CODE ANN. § 39-14-150(g) (2011); TEX. BUS. & COM. CODE § 521.053 (2010); UTAH CODE § 13-37-201; VT. STAT. ANN. tit. 9, § 2445 (2011); WASH. REV. CODE § 19.215.020(1) (2011); WIS. STAT. § 137.97(2) (2010); 2005 R.I. Pub. Laws 225 (2008); H.B. 5694 § 1, Reg. Sess. (Conn. 2009); S.B. 2292 § 2, 23rd Leg., Reg. Sess. (Haw. 2006); S.B. 196, 81st Leg., Reg. Sess., (Kan 2005); S.B. 583, 74th Leg., Reg. Sess. (Or. 2007).

236. *See* KY. REV. STAT. ANN. § 365.725.

237. *Id.*

238. ARK. CODE ANN. § 4-110-104(b); CAL. CIV. CODE § 1798.81-5; NEV. REV. STAT. § 603A.210

require businesses that hold personal information to implement “reasonable security procedures . . . appropriate to the nature of the information.”<sup>239</sup> All of the statutes use this “reasonable” language, which is not defined, mirroring the approach taken by the FTC in its Red Flags Rule.<sup>240</sup>

### 3. *Financial Information Statutes*

States have stepped up to protect financial information as well, and in many cases, go further than federal law.<sup>241</sup> California is a good example of a state that has myriad laws on financial privacy. These laws include the state’s Financial Information Privacy Act (“FIPA”),<sup>242</sup> which in some ways mirrors the Gramm-Leach-Bliley Act but which has more protection for customers.<sup>243</sup> Unlike Gramm-Leach-Bliley,<sup>244</sup> FIPA requires customers to “opt-in” before businesses can share their information with third parties.<sup>245</sup> California also prevents disclosure of bookkeeping records<sup>246</sup> and tax returns.<sup>247</sup>

### 4. *Internet-Specific Legislation*

Some states also have a host of laws that specifically protect information collected over the Internet. California requires all websites that collect personally identifiable information on state residents to “conspicuously post” a privacy policy on their website.<sup>248</sup> Willful or

(2009); TEX. BUS. & COM. CODE § 521.053; UTAH CODE § 13-44-201 (2011); 2005 R.I. Pub. Laws 225; S.B. 583, 74th Leg., Reg. Sess. (Or. 2007).

239. ARK. CODE ANN. § 4-110-104(b).

240. See 12 C.F.R. § 222.90 (2010).

241. KENNEDY, *supra* note 5, at 70.

242. CAL. FIN. CODE §§ 4050–4060 (2010).

243. WOLF, *supra* note 184, § 2:9.3[A], at 2-83.

244. See 15 U.S.C. § 6802 (2006) (giving customers the option to opt-out of third-party sharing).

245. See CAL. FIN. CODE § 4052.5. FIPA also gives customers the ability to opt-out of sharing with affiliates and subsidiaries. *Id.* § 4052.5(b)(1). The Ninth Circuit, however, ruled that this provision is largely preempted by federal law. See *Am. Bankers Ass’n v. Lockyer*, 541 F.3d 1214, 1216 (9th Cir. 2008).

246. CAL. CIV. CODE § 1791.1 (2010).

247. *Id.* § 1799.1.

248. CAL. BUS. & PROF. CODE § 22575(a) (2010). The privacy policy must:

- (1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.
- (2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.
- (3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator’s privacy policy for that Web site or online service.
- (4) Identify its effective date.

negligent violation of the posted policy is a violation of the statute.<sup>249</sup> Two states require Internet service providers to keep their customers' personal data private.<sup>250</sup> California has a law that prohibits spyware,<sup>251</sup> and at least thirteen other states have followed California's lead with similar antispyware provisions.<sup>252</sup>

These state laws are spotty, sometimes provide limited protection, and often contain worrisome loopholes. The encryption safe harbors are particularly difficult to justify. However, these laws provide a good start in addressing the real concerns of data collection. The data protection statutes provide a possible framework for broader minimum security standards that could be adopted by the FTC. And when it comes to laws that govern the Internet, most companies are likely to adopt more stringent state standards for fear of being sued under the strictest state laws. However, undoubtedly there would be better protection and greater certainty for business if the federal government were to institute more uniform laws in these areas.

## V. WORKING TOWARD A SOLUTION

As discussed above, any common law solution to the problems posed by databases of personal information appears to be limited. Congressional and state action have been helpful, but so far inadequate. While there have been a multitude of statutes passed in recent years that seek to address the problems of identity theft and the inappropriate collection and use of personal information, the result has been a smattering of overlapping laws that contain significant holes. The fact that large categories of private information and businesses are not covered by any law is particularly worrisome.

While it would seem that a radical solution is needed to deal with this very real and growing problem, this Note takes a more moderate position. This Note proposes that Congress create limited classes of information that are zealously protected, that the FTC come up with a better system to protect customers from the most unsavory business practices, and that states and the FTC do more to protect personal

---

*Id.* § 22575(b).

249. *Id.* § 22576. The statute does not contain an enforcement provision; however, it is likely that there is a private right of action under California's Unfair Competition Law. *See WOLF, supra* note 184, § 5:2.1[A], at 5-11; *see also* CAL. BUS. & PROF. CODE §§ 17200-17210 (2010).

250. Minnesota protects "information that identifies: (1) a consumer by physical or electronic address or telephone number; (2) a consumer as having requested or obtained specific materials or services from an Internet service provider; (3) Internet or online sites visited by a consumer; or (4) any of the contents of a consumer's data-storage devices." MINN. STAT. ANN. § 325M.01(5) (West Supp. 2010). Nevada's statute protects "all information" other than email addresses, which must be kept confidential at the customer's request. NEV. REV. STAT. § 205.498(1)(a) (2009).

251. CAL. BUS. & PROF. CODE §§ 22947-22947.6 (2010).

252. *See WOLF, supra* note 184, § 5:3.2, at 5-15.

information from being stolen or lost. Most of these changes could be implemented by broadening laws already in place and following the best state practices.

There are several reasons that these changes would be best implemented by the legislative branch and federal administrative agencies, rather than by the courts. First is the recognition that this is a rapidly developing area of business and technology. Heavy-handed court decisions could destroy the legitimate and productive uses of the vast quantity of information produced in our information-saturated world.<sup>253</sup> Second is the hope that allowing Congress and regulatory agencies to decide how to proceed will produce more carefully crafted and—hopefully—cautious rules. Third, Congress and administrative agencies represent the branches of government that are arguably best equipped to make policy decisions about how better to protect the privacy interests of Americans without harming business.

This Note proposes that the problem be broken into four parts: (1) collection of private data, (2) the internal use of private data, (3) the sale or rental of personal data, and (4) keeping data in an insecure manner that exposes it to loss and theft. Each of these activities presents different problems and requires tailored solutions.

#### A. DATA COLLECTION

Companies collect data in the regular course of business. This is true in all but anonymous cash-only transactions. Paying with a credit card, ordering by mail or through the Internet, or establishing almost any relationship with a business is bound to leave a record of the customer's name and address, at least. The deeper the relationship, the more data is likely to be collected and stored. Banks, healthcare providers, accountants, and lawyers have detailed information on their customers. Employers also have vast amounts of information about their employees.

This sort of data collection and storage seems unavoidable. Simply conducting normal business activities will produce these records. These records are largely needed by the companies collecting them; laws limiting collection would likely be burdensome and difficult to comply with. Still, some regulation in this area is appropriate.

---

253. Courts are particularly bad at understanding even the basics of technology. The oral argument in *City of Ontario v. Quon* provides a particularly striking example. *See generally* Transcript of Oral Argument, *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010) (No. 08-1332). During the hearing, several Supreme Court Justices made comments that revealed how little they knew about text messages and email. For example, Justice Scalia wondered if text messages could be printed out “and circulated”—apparently unaware of the concept of forwarding. *Id.* at 49. Justices Kennedy and Roberts did not understand what would happen if one were to send a text message at the same time one received one. Kennedy asked if you would get a voicemail message. *Id.* at 44.

The Children's Online Privacy Protection Act is an example of a law that identifies a narrow exception to the general rule that almost any collection of information in a business context should be allowed.<sup>254</sup> With this Act, Congress reasonably determined that businesses should be forced to get a parent's permission before collecting information on children.<sup>255</sup> While the Act has the unfortunate problem of providing little guidance on which websites are covered by the law,<sup>256</sup> it is exactly the type of limitation on collection that will protect a vulnerable population without being overly burdensome on businesses. Similarly appropriate restrictions on collection are the Computer Fraud and Abuse Act<sup>257</sup> and various state spyware statutes.<sup>258</sup> These laws identify activities that are not simply information collection, but intrusions into private space. Legislatures have correctly recognized the difference between collecting information in arms-length transactions and collecting information by invading a person's computer without her permission.

The Cable Communications Policy Act<sup>259</sup> also contains limits on the collection of information. While the goal of ensuring the privacy of what one watches in her home is important, legislatures should be careful before extending the Act's collection restrictions into other areas, such as the Internet. While the sharing of Internet browsing and search information should be better regulated,<sup>260</sup> the initial collection and internal use of that information is vital to many companies. Regulating the collection of such information should be done only in the most extreme circumstances, with the presumption being that data collection should be almost universally allowed.

The default position in all areas should be to permit the collection of information. Regulating collection alone would likely create difficulty in enforcement and in line drawing. While other data-handling practices should be more tightly regulated, collection alone is not the best place to control the behavior of private data usage.

#### B. INTERNAL DATA USE

Once data is collected, it is often used for legitimate business purposes by the companies that collect it. This has been going on for decades<sup>261</sup> and has only accelerated with the introduction of high-powered computing.<sup>262</sup> Companies use the extensive data they collect in

---

254. See 15 U.S.C. §§ 6501–6506 (2006).

255. *Id.*

256. KENNEDY, *supra* note 5, at 14–15.

257. 18 U.S.C. § 1030 (2006).

258. See *supra* Part IV.C.4.

259. 47 U.S.C. § 551 (2006).

260. See *infra* Part V.C.

261. See SOLOVE, *supra* note 2, at 16–17.

262. Lohr, *supra* note 5, at BU3.

remarkable ways. Canadian Tire uses data from its credit card customers to determine whether or not they are likely to repay their loans.<sup>263</sup> AT&T uses demographic data to predict the amount of traffic that each subscriber adds to its cellular network.<sup>264</sup> For some Internet companies, customer data provides the basis for ads that generate much of their revenue.<sup>265</sup>

It has been shown time and again that this information, if used responsibly, can have surprising social benefits. For example, Google search queries have been used to accurately track flu outbreaks.<sup>266</sup> Google accurately estimates the level of flu activity in a region with a lag time of just one day.<sup>267</sup> This sort of capability would have been extremely difficult to predict when Google was launched and would likely be much more difficult if laws such as the Do Not Track list were enacted.

The in-house use of collected information is vital to many industries and should not be infringed upon. As long as there are adequate protections against the alienation and loss of data, the government should be cautious in any attempt to regulate the internal use of information legally collected by companies.

However, the definition of “internal use” must be addressed. While allowing almost unfettered use of internal data should be the default position of lawmakers, subsidiaries and affiliated organizations should not always be treated as the same organization. With the consolidation of companies in general—and high-tech Internet companies in particular—perhaps opt-out provisions like those in California should be considered. When it comes to sharing among affiliates and subsidiaries, opt-out provisions protect the most sensitive customers while still protecting business interests. The most sensitive customers can simply opt-out of

---

263. Charles Duhigg, *What Does Your Credit-Card Company Know About You?*, N.Y. TIMES, May 17, 2009, at MM40. The company figured out that

people who bought cheap, generic automotive oil were much more likely to miss a credit-card payment than someone who got the expensive, name-brand stuff. People who bought carbon-monoxide monitors for their homes or those little felt pads that stop chair legs from scratching the floor almost never missed payments. Anyone who purchased a chrome-skull car accessory or a ‘Mega Thruster Exhaust System’ was pretty likely to miss paying his bill eventually.

*Id.*

264. Niraj Sheth, *AT&T Prepares Network for Battle*, WALL ST. J., Mar. 31, 2010, at B1.

265. See Claire Cain Miller, *Twitter Unveils Plans to Draw Money from Ads*, N.Y. TIMES, Apr. 12, 2010, at B1 (discussing Twitter’s plan to sell advertising based on searches); see also Jefferson Graham, *Businesses Turn to Facebook for Word-of-Mouth Advertising*, USA TODAY, Aug. 5, 2009, at 7A (“You can target your ad better on Facebook than anywhere else. I know my customers’ age, where they live, what their interests are, and only the people who fit my target see the ads.” (quoting Facebook advertiser Cam Balzer)).

266. Jeremy Ginsberg et al., *Detecting Influenza Epidemics Using Search Engine Query Data*, 457 NATURE 1012, 1012 (2009).

267. *Id.* at 1014.

any affiliate sharing programs while businesses will be content knowing that the vast majority of their customers will not take the step to opt-out.

### C. INFORMATION SALE AND RENTAL

The sale and rental of personal information to third parties is troubling, but legislatures and regulators must approach restrictions with care. The sale and rental of data is a large business that many companies depend on for sales and marketing information.<sup>268</sup> The best approach would be one that largely preserves the status quo while putting a stop to the worst practices of the industry. This can be done through an extension of laws already in place.

As it stands, most laws that limit which information can be disseminated to third parties focus on the type of information involved. These laws seek to protect information that Congress or state legislatures deem too private to share. Many of these laws protect financial information by limiting which information can be shared and with whom. Other laws create total or near-total bans on dissemination of certain kinds of information. These types include information on a person's health,<sup>269</sup> video rental activities,<sup>270</sup> television watching,<sup>271</sup> and communications.<sup>272</sup> Whether by design or by chance, these particular types of information are more personal than unprotected information. One's media consumption habits, bank statements, and communications have the potential to reveal one's inner thoughts and bodily condition. They are the sort of private information we would be unwilling to give to all but our closest friends and family members. This rationale could easily be extended to Internet searches, website histories, information uploaded to social networking sites, or mobile phone location and usage information. In 2006, America Online released twenty million of its members' Internet search queries as part of a research project.<sup>273</sup> Looking at these search histories gives you the feeling of being inside someone's head. The thoughts and feelings of the individual can easily be discerned from the searches.<sup>274</sup> The searches show everything from the user's interests in

---

268. SOLOVE, *supra* note 2, at 1.

269. *E.g.*, 42 U.S.C. § 201 (2006); 45 C.F.R. 164.501 (2010).

270. 18 U.S.C. § 2710 (2006).

271. 47 U.S.C. § 551 (2006).

272. 12 C.F.R. § 222(c)(1) (2010).

273. Declan McCullagh, *AOL's Disturbing Glimpse into Users' Lives*, CNET, Aug. 7, 2006, [http://news.cnet.com/AOLs-disturbing-glimpse-into-users-lives/2100-1030\\_3-6103098.html](http://news.cnet.com/AOLs-disturbing-glimpse-into-users-lives/2100-1030_3-6103098.html).

274. A CNET reporter combed the AOL search data and found some fairly disturbing examples of just how personal one's Internet search history can be. *Id.* ("AOL user 9486162 appears to live near Edisto Beach, S.C., and could be a poker aficionado who's a fan of the University of Kentucky's football team. User 9486162 rarely used his or her AOL account for searching in March, but was preoccupied with one disturbing topic on April 26: university of kentucky football; hold'em poker school; ways to kill yourself; suicide by natural gas; how to kill oneself by natural gas; assisted suicide; suicide by overdosing; how long does carbon monoxide poisoning take to kill a person; over dose ways

particular sports teams to thoughts of suicide.<sup>275</sup> The rationale that some information is so private that it essentially offers a window into a person's mind and thus should not be shared was behind the passage of the Video Privacy Protection Act, which bans the dissemination of video rental history.<sup>276</sup>

Senator Paul Simon's comments in May 1988 about the Video Privacy Protection Act could easily be mistaken for criticism of the kind of high-tech data collection being done today:

There is no denying that the computer age has revolutionized our world. Over the past 20 years we have seen remarkable changes in the way each one of us goes about our lives. Our children learn through computers. We bank by machine. We watch movies in our living rooms. These technological innovations are exciting and as a nation we should be proud of the accomplishments we have made.

Yet, as we continue to move ahead, we must protect time honored values that are so central to this society, particularly our right to privacy. The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to be more intrusive than ever before. Every day Americans are forced to provide to businesses and others personal information without having any control over where that information goes. These records are a window into our loves, likes, and dislikes.<sup>277</sup>

The Video Privacy Protection Act came about after the *Washington City Paper* published the video rental records of then-Supreme Court nominee Judge Robert Bork.<sup>278</sup> The Act was introduced less than a month later.<sup>279</sup>

There's a gut feeling that people ought to be able to read books and watch films without the whole world knowing. Books and films are the intellectual vitamins that fuel the growth of individual thought. The whole process of intellectual growth is one of privacy—of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye.<sup>280</sup>

---

to commit suicide; university of kentucky 2007 football recruits; texas hold'em poker on line seminars; employment needed—louisville ky"). The CNET article also revealed the search history of someone searching for child porn, someone looking to get revenge on a boyfriend, and a woman struggling with self-image issues and pregnancy. *Id.*; see also Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1 (showing how easy it is to figure out the true identity of a supposedly anonymous user by analyzing her search information).

275. McCullagh, *supra* note 274.

276. 18 U.S.C. § 2710 (2006).

277. S. REP. NO. 100-599, at 6-7 (1988) (quoting 134 CONG. REC. S5401 (daily ed. May 10, 1988) (statement of Senator Paul Simon)).

278. Michael Dolan, *The Bork Tapes*, WASH. CITY PAPER, Sept. 25-Oct. 1, 1987, at 1; see also *Editorial: Invasion of Video Privacy*, WASH. POST, Sept. 30, 1987, at A18.

279. Dennis McDougal, *Video Rental Privacy Bill Introduced*, L.A. TIMES, Oct. 23, 1987, at 1 (Calendar).

280. S. REP. NO. 100-599, at 7 (statement of Rep. Alfred McCandless).

These sentiments are even more true when it comes to the Internet. Would the reaction to the release of a prominent public official's Internet search and browsing history be any different than the reaction to the release of Bork's video rental history? If anything, it would likely be worse.

This is not to say that such information should not be collected or used by the companies that collect it. Much of the Internet search industry relies on this information to better hone its search capabilities. However, this information should not be shared. As Congress recognized with the Video Privacy Act, there is some information that is simply too personal to be disseminated.

Banning the sale and rental of private information is not a perfect solution, but it provides the best balance between privacy and business innovation. Allowing companies virtually unfettered use of the data they collect allows them to continue to innovate. Banning the dissemination of that data, however, keeps it contained. This containment has several benefits. First, it allows the customer or web surfer to know that her data will be available only to companies that she does business with or visits. This presumably will give those concerned about the spread of their private information the reassurance that—at the very least—it will be available only to those they trust enough to give it to in the first place. Second, if such a ban were coupled with more stringent data security laws, it would create some assurance that the collector of that data is responsible for keeping it safe and is unable to share it with another person or entity that might not be as careful. Third, a ban makes it less likely that separate strands of data will be pieced together to discover personal information about a person that she had no intention of sharing. For example, it would prevent a data broker from combining GPS information from a mobile phone company with credit card purchase histories to map out a customer's shopping route and determine what she looked at before she made a purchase. This reduces the danger to personal privacy posed by "digital dossiers," because they would be much harder to assemble.

#### D. DATA THEFT

There are two ways to attack the problem of data theft. Laws can try either to prevent data theft before it happens, or to prevent further harm to those whose data has been compromised. Current state and federal law, as well as regulations promulgated by the FTC, could be much more robust in both of these areas.

On data loss prevention, the FTC's Red Flags Rule could be much more robust. Considering that the objective is to protect private information being held by more than just financial and credit-giving companies, the rule should be extended to all businesses that hold such

information. A Red Flags Rule that more closely resembles state statutes<sup>281</sup> in this area would be helpful. The FTC should place *any business* that holds private information under a duty to use reasonable measures to safeguard that data, because companies that are not defined as financial institutions or credit-giving hold vast quantities of information. In fact, many would argue that the information held by institutions, such as Internet search engines, is more private than the information held by financial institutions. While the loss of private financial information could be damaging in terms of dollars and cents, the privacy implications of the loss of what amounts to private thoughts and interests is much more invasive.

Laws protecting customers once their data has been released are much more effective than the FTC's current regulations, but could be improved. As it stands, most states give companies safe harbor from breach notification laws if they use encryption technology.<sup>282</sup> But whether the data is lost or stolen from an encrypted system or from a nonencrypted one, the customers' data is just as vulnerable. If the objective is to give notice to customers that their data has been compromised, it should not matter how the data was stored before it was stolen. This is not to say that there should be no incentives for companies to encrypt their data or to promote best practices, but notification laws should not be used to provide such incentives. Safe harbors might be better used to protect companies from lawsuits or regulatory action. There also is no good reason to limit notification laws to information stored on computers. Only two states require notification if the stolen data was not kept on a computer, and only one of those two requires no tie to a computer for breach notification to be mandatory.<sup>283</sup> Again, if the purpose of notification laws is to alert potential identity-theft victims that their data has been compromised, laws must be expanded to include all data breaches, no matter how the information is stored.

Notification laws, however, are inadequate without satisfactory protection from theft in the first place. Once the information is out, it is often up to the consumer to make sure the proper steps are taken to protect their identity. That is why there must be more stringent protections on data: so it is less likely to be stolen in the first place.<sup>284</sup> Stronger protections, in conjunction with adequate notification laws,

---

281. ARK. CODE ANN. § 4-110-104(b) (2011); CAL. CIV. CODE § 1798.81.5 (2010); NEV. REV. STAT. § 603A.210 (2009); TEX. BUS. & COM. CODE § 521.053 (2010); UTAH CODE § 13-44-201 (2011); 2005 R.I. Pub. Laws 225 (2008); S.B. 583, 74th Leg., Reg. Sess. (Or. 2007).

282. See, e.g., CAL. CIV. CODE § 1798.82(a) (2010).

283. CONN. GEN. STAT. § 36a-701b (2011).

284. Data theft prevention might be accomplished through a more stringent FTC Red Flags Rule, which could require better information protection practices such as the mandatory use of encryption technology.

would go a long way toward limiting this growing financial and privacy threat.

#### E. A CONSTITUTIONAL LIMITATION

Any proposed solution to the problem of data sales must confront the limitations imposed by the First Amendment. As discussed in relation to the tort of public disclosure, the First Amendment restricts the ability of legislatures to limit the dissemination of truthful information.<sup>285</sup> This limitation was on display most recently in *Sorrell v. IMS Health Inc.*, in which the Court struck down a limitation on the use and dissemination of prescription drug information, holding that the ban was an unconstitutional limitation on commercial speech.<sup>286</sup>

Two aspects of the Vermont statute at issue in *Sorrell* raised constitutional problems. First, it barred the sale of prescription information to those who would use it for marketing purposes. The Court held this to be a content-based restriction because it singled out a particular disfavored type of speech—marketing.<sup>287</sup> Second, the law barred pharmaceutical manufacturers from using the information for marketing purposes. The Court held that this limitation was speaker-based because it singled out a disfavored speaker—pharmaceutical manufacturers.<sup>288</sup> Because the law contained content- and speaker-based restrictions, the Court imposed heightened scrutiny, requiring the government to show that the law “directly advance[d] a substantial governmental interest and that the measure [was] drawn to achieve that interest.”<sup>289</sup> Vermont argued that the statute was “necessary to protect medical privacy,” but this justification did not withstand heightened scrutiny.<sup>290</sup> The Court suggested that the need for privacy could well be a substantial interest but that the statute was “not drawn to serve that interest.”<sup>291</sup> The law allowed for wide dissemination of prescription information—for health care research, for example—to a large number of individuals, including “insurers, researchers, journalists, and the state itself.”<sup>292</sup> Thus, because of the “information’s widespread availability and many permissible uses,” the “asserted interest in physician confidentiality [did] not justify the burden [the statute] places on protected expression.”<sup>293</sup>

---

285. *See supra* Part I.B.

286. No. 10-779, slip. op. at 1 (U.S. June 23, 2011).

287. *Id.* slip op. at 8.

288. *Id.*

289. *Id.* slip op. at 15–16.

290. *Id.* slip op. at 17. The State also argued that the statute was integral to improving public health and reducing healthcare costs. *Id.*

291. *Id.* (“It may be assumed that, for many reasons, physicians have an interest in keeping their prescription decisions confidential.”).

292. *Id.*

293. *Id.* slip op. at 3.

However, in the majority opinion Justice Kennedy left the door open for some laws that restrict companies from disclosing personal information. He did so by first noting the danger posed by data storage in the computer age:

The capacity of technology to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests, however, the State cannot engage in content-based discrimination to advance its own side of a debate.<sup>294</sup>

He then hinted that Vermont's law might have passed constitutional muster if it had "provided that prescriber-identifying information could not be sold or disclosed except in narrow circumstances."<sup>295</sup> In doing so, Kennedy cited the Health Insurance Portability and Accountability Act, which is one of the models this Note suggests building upon to protect a wider array of private information.<sup>296</sup>

In *Sorrell*, the Court suggested strongly that personal privacy can be a substantial government interest.<sup>297</sup> Furthermore, Justice Kennedy seems to leave open the possibility that general bans on the dissemination of personal information while allowing a "few narrow and well-justified" exceptions would advance that interest.<sup>298</sup> That is precisely what this Note recommends.

#### F. COMPETING PROPOSALS

Recently, there have been two high-profile proposals seeking to curtail the threat to individual privacy that the Internet poses. First, the FTC proposed a so-called "Do Not Track" scheme whereby individuals could opt out of online tracking, most likely through the use of software installed on their computer.<sup>299</sup> Second, Senators John Kerry and John McCain have begun distributing a working draft of the "Commercial Privacy Bill of Rights Act of 2011," a rather comprehensive proposal that would address data security, data use, and data collection.<sup>300</sup> However, both of these proposals have shortcomings that make them less appealing than the solution this Note proposes.

---

294. *Id.* slip op. at 24.

295. *Id.* slip op. at 24–25.

296. *Id.* slip op. at 18.

297. *Id.* slip op. at 24.

298. *Id.* slip op. at 18.

299. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 63–67 (2010) [hereinafter FTC, PROTECTING CONSUMER PRIVACY].

300. John L. Kerry & John S. McCain, *Staff Working Draft of the Commercial Privacy Bill of Rights Act of 2011*, KERRY.SENATE.GOV (Mar. 11 2011), <http://kerry.senate.gov/imo/media/doc/Commercial%20Privacy%20Bill%20of%20Rights%20Text.pdf>.

### I. Do Not Track

Recently, the FTC lobbied Congress to enact so-called “Do Not Track” legislation.<sup>301</sup> Since then, H.R. 654 has been introduced.<sup>302</sup> This bill would allow any web user to choose whether or not online companies could collect information about their Internet use.<sup>303</sup> Such a law has been compared to the successful “Do Not Call” list established in 2003,<sup>304</sup> but the mechanism would likely be quite different.<sup>305</sup> Users would probably set a preference on their web browser or use a piece of software that would signal to websites that they have opted out of data collecting.

The Do Not Track list is a substantial break with the FTC’s previous efforts to protect customers’ private information. In the past, the FTC has used enforcement actions to protect customers’ private information.<sup>306</sup> In the 1990s, the FTC relied chiefly on the concept of “notice and choice,”<sup>307</sup> which looks at whether the consumer has been given adequate notice as to how their information has been collected and the choice whether or not to be involved.<sup>308</sup> Since the early 2000s, the Commission has used the “harm-based approach,” which focuses on whether there was any actual harm done to the consumer.<sup>309</sup> This harm-based approach, however, does not take into account intangible harms, a serious drawback.<sup>310</sup> To its credit, the FTC has rejected these past frameworks, which have proven to be inadequate in protecting consumers’ private information. The FTC has recognized that the notice and choice model led only to long, increasingly difficult-to-understand notices that were of little help to the average web user.<sup>311</sup> The harm-based approach is not any better. The FTC now recognizes that much of the harm done by data collection and dissemination is “reputational harm, as well as the fear of being monitored or simply having private information ‘out there.’”<sup>312</sup>

---

301. See *Prepared Statement of the FTC on Do Not Track: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection*, 112th Cong. (2010) (statement of David Vladeck, Director of the Bureau of Consumer Protection of the FTC).

302. H.R. 654, 112th Cong. (2011).

303. *Id.*

304. See Edward Wyatt & Tanzina Vega, *FTC Backs Plan to Honor Privacy of Online Users*, N.Y. TIMES, Dec. 1, 2010, at A1.

305. The proposed law does not spell out how users would be able to opt-out of data collection, something that would be left to FTC rulemaking.

306. See, e.g., *In re Sears Holdings Mgmt. Corp.*, F.T.C. File No. 0823099 (Aug. 31, 2009).

307. FTC, *PRIVACY ONLINE: A REPORT TO CONGRESS 7–9* (1998).

308. David Vladeck, Director FTC Bureau of Consumer Protection, *The Role of the FTC in Consumer Privacy Protection at the International Association of Privacy Professionals Practical Privacy Series 2* (Dec. 8, 2009), *transcript available at* <http://www.ftc.gov/speeches/vladeck>.

309. *Id.* at 3.

310. The harm-based approach looked for “physical harm, economic harm in the form of identity theft or denial of credit, or unwarranted intrusions into people’s daily lives.” *Id.*

311. See FTC, *PROTECTING CONSUMER PRIVACY*, *supra* note 299, at 19–20.

312. *Id.* at 20.

The Do Not Track legislation is not the answer to these problems. The proposal goes both too far and not far enough. First, it goes too far in that it will severely limit what a collector of information can do with it. As noted in Part V.B above, this is a somewhat drastic measure to take. The in-house use of collected information is the lifeblood of the information age and of many high-tech companies.<sup>313</sup> The law does have exceptions including any “category of operational use specified by the Commission by regulation that is consistent with the purposes [of the law].”<sup>314</sup> But the extent of these exceptions will be left largely to the interpretation of the FTC and subject to lawsuits. Such uncertainty is exactly the sort of thing that should be avoided if the United States is to maintain a healthy high-tech industry. Second, Do Not Track does not go far enough because it requires users to opt out. Most users are unlikely to do so. Opt-out provisions create an extra step that many unsophisticated users will not understand or know how to implement. Those users who are most at risk for privacy invasion are those who are the least technically proficient and the least likely to opt out. These are often the elderly or others with limited technical abilities.<sup>315</sup> A more sensible solution would be to allow data collection and protect privacy through other means.

## 2. *Privacy Bill of Rights*

The “online privacy bill of rights,” as currently proposed, would require data collectors to: (1) establish “reasonable security measures” to protect their data; (2) give individuals notice regarding the “collection, use, transfer, or maintenance” of the data collected about them; (3) require opt-in consent for the “collection, use, or transfer of sensitive personally identifiable information other than to process a transaction or service requested by that individual or for fraud prevention . . . or to provide for a secure environment”; (4) allow individuals to inspect and correct any information possessed about them; (5) collect only as much information as they need and retain that information only as long as needed; and (6) require all third parties with whom they share information to maintain it just as the collector would, and require that

---

313. Ron A. Dolin, *Search Query Privacy: The Problem of Anonymization*, 2 HASTINGS SCI. & TECH. L.J. 137, 142–48 (2010).

314. H.R. 654, 112th Cong. § 3(d)(7) (2011).

315. An example of just how unsophisticated many elderly users are comes from America Online’s customer base. AOL still derives a substantial portion of its profits from customers who pay for dial-up Internet access. Most of these users already have high-speed DSL or cable service but do not know they can stop paying AOL twenty-five dollars a month. Ken Auletta, *You’ve Got News*, NEW YORKER, Jan. 24, 2011, at 32. “The dirty little secret,” a former AOL executive told the New Yorker, “is that seventy-five per cent of the people who subscribe to AOL’s dial-up service don’t need it.” *Id.* It is unlikely that millions of online users like those who still use AOL would be sophisticated enough to understand the privacy implications of data collection, let alone how to properly opt-out.

the third party not combine the information with information from other sources in order to identify particular individuals.<sup>316</sup>

There are at least two praiseworthy proposals in the draft legislation. First, the online bill of rights targets data security, collection, use, and dissemination all at once<sup>317</sup>—a feature almost unique in data protection legislation. The comprehensive nature of the legislation would be greatly appreciated by businesses that are now forced to follow myriad state and federal laws covering all of these issues independently. Second, the online bill of rights would prompt the FTC to establish better security rules for businesses. While the online bill of rights leaves almost all of the specifics to the FTC, it does provide the Commission with a chance to improve upon the flawed Red Flags Rule.

However, the proposal fails in a number of ways. First, the notice and correction provisions, while interesting, are unlikely to provide any help to consumers. These notices will not likely be any clearer or more helpful than the complicated and rarely used notices already required by banks and other financial institutions. Such notice requirements will only add burdens to business without actually helping to prevent the most invasive practices of data collectors.

Second, the opt-in provision is worrying in several respects. The draft legislation requires individuals to opt-in even for the collection of “sensitive personally identifiable information.” The proposal defines this as “personally identifiable information which, if lost, compromised or disclosed without authorization could result in harm to an individual.”<sup>318</sup> The word “harm” is never defined. If “harm” includes emotional or reputational harm, it would include almost any piece of information that could cause someone emotional difficulty. If “harm” does not include emotional harm, the legislation is no better than the harm-based approach tried and rejected by the FTC. The opt-in requirement also is likely to do real harm to businesses. Even those who do not mind having their personal information collected are unlikely to give an institution affirmative permission to track them. Without this information, Internet companies in particular are going to lose a valuable source of income. Senator Claire McCaskill, a Missouri Democrat, expressed worries that these restrictions could hinder the ability of websites to provide free content: “I just want to make sure that we don’t kill the goose that laid the golden egg,” she told the *Wall Street Journal*.<sup>319</sup> There is no reason to

---

316. The proposal would not apply to all collectors. Instead, it would apply only to entities collecting information on 5000 individuals during a twelve month period, and only to those entities that meet other requirements listed in the proposal. John L. Kerry & John S. McCain, *Staff Working Draft of the Commercial Privacy Bill of Rights Act of 2011*, KERRY.SENATE.GOV (Mar. 11 2011), <http://kerry.senate.gov/imo/media/doc/Commercial%20Privacy%20Bill%20of%20Rights%20Text.pdf>.

317. Kerry & McCain, *supra* note 316, § 202(a)(1)(A).

318. *Id.* § 3(5).

319. Jennifer Valentino-DeVries, *Privacy Measure Attracts Support*, WALL ST. J., Mar. 17, 2011, at B1.

go this far. Simply requiring data collectors to keep personal data safe and prohibiting them from selling it to others would provide much-needed protection while also allowing some of the world's most innovative companies to stay in business. The solution proposed by this Note strikes this balance and provides a simple rule that businesses could easily follow.

#### CONCLUSION

The problem of data collection and dissemination is real, but courts and legislatures should be cautious in how they go about solving it. Courts should be especially cautious in using privacy torts, breach of confidence, or any property rights to address the problem. Doing so would expand those doctrines far beyond their breaking point. Instead, legislatures and administrative agencies should carefully address the most troublesome privacy concerns with well-targeted, limited laws and regulations. This may well include expanding the categories of information subject to heightened protection and strengthening laws designed to prevent identity theft. As information becomes more readily available and easier to transmit, the data-collection problem will only become more acute. Regulators and lawmakers need to recognize this fact and move quickly toward more enhanced protections—including a ban on the sale of private information.