MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 37 | Issue 4 Article 12

2011

Putting the Genie Back in the Bottle: Leveraging Private Enforcement to Improve Internet Privacy

Jonathan D. Frieden

Charity M. Price

Leigh M. Murray

PUTTING THE GENIE BACK IN THE BOTTLE: LEVERAGING PRIVATE ENFORCEMENT TO IMPROVE INTERNET PRIVACY

Jonathan D. Frieden, Esq.[†]

Charity M. Price, Esq.[††]

Leigh M. Murray, Esq.[†††]

I. INTRODUCTION 1673
II. CURRENT PROTECTIONS 1675
A. *The Federal Trade Commission* 1675
1. *A Historical Look at the FTC's Approach to Internet Privacy* 1676
2. *The FTC's Privacy Enforcement Actions* 1677
3. *The Future of the FTC's Involvement* 1682
B. *Federal Statutes* 1683
1. *The Children's Online Privacy Protection Act* 1683
2. *The Electronic Communications Privacy Act* 1687
3. *Pending Legislation* 1688
C. *State Statutes* 1690
1. *California* 1690
2. *Connecticut* 1692
3. *Minnesota* 1693
4. *Nebraska* 1694
5. *Nevada* 1694
6. *New York* 1696
7. *Pennsylvania* 1696

† Principal, Odin, Feldman & Pittleman, P.C., Fairfax, Virginia. B.A., 1994, University of Virginia; J.D., 1997, University of Richmond, T.C. Williams School of Law.

†† Associate, Odin, Feldman & Pittleman, P.C., Fairfax, Virginia. B.A., 2004, Wellesley College; J.D., 2009, George Washington University Law School.

††† Associate, Odin, Feldman & Pittleman, P.C., Fairfax, Virginia. B.A., 2005, The Pennsylvania State University; J.D., 2010, American University, Washington College of Law.

8. Utah 1697
9. Virginia 1698
10. Wisconsin 1699
III. COMPARABLE PROTECTIONS IN FOREIGN NATIONS 1700
A. European Union 1700
B. United Kingdom 1703
C. Canada 1704
IV. PRIVATE ENFORCEMENT OF INTERNET PRIVACY PROTECTIONS THROUGH LITIGATION 1706
A. DoubleClick 1706
B. Intuit 1707
C. Pharmatrak 1708
D. Post-9/11 Airline Cases 1710
1. Northwest Airlines 1710
a. Minnesota 1711
(1) ECPA Claim 1711
(2) FCRA Claim 1712
(3) Deceptive Trade Practices and Negligent Misrepresentation Claims 1713
(4) Trespass Claim 1713
(5) Intrusion upon Seclusion Claim 1714
(6) Breach of Contract and Warranty Claims 1714
*b. North Dakota (*Dyer v. Northwest Airlines*)* 1715
(1) ECPA Claim 1716
(2) Breach of Contract Claim 1716
2. American Airlines 1717
a. ECPA Claim 1717
b. Breach of Contract Claim 1718
c. State Law Claims 1718
3. JetBlue 1719
a. ECPA Claim 1720
b. Violation of New York General Business Law 1720
c. Breach of Contract Claim 1721
d. Trespass to Property 1721
e. Unjust Enrichment 1722
V. NEW LEGISLATION SHOULD LEVERAGE PRIVATE ENFORCEMENT MECHANISMS 1722
VI. CONCLUSION 1726

"Privacy is Dead. Get Over It. You can't put the genie back in the bottle."[1]

—Steve Rambam

I. INTRODUCTION

> More than ever before, our lives are visible to others, from government agencies and security services to the owners of the websites we surf and the stores where we shop. They track us in public, in workplaces and online, compiling our personal information in massive databases and sorting us into categories of risk, value and trustworthiness.[2]

Shockingly, a significant portion of the information about us which is visible to others is *made visible by us*.[3]

Two hundred forty million Americans use the Internet.[4] We shop online,[5] make online travel reservations,[6] bank online,[7] visit government websites,[8] use social media websites,[9] and engage in a myriad of other Internet transactions. In doing so, we reveal our

1. Robert L. Mitchell, *The Grill: Privacy Is a Thing of the Past, Says Private Investigator*, COMPUTERWORLD (Oct. 10, 2008, 12:00 PM), http://www.computerworld.com/s/article/326821/The_Grill_Privacy_is_a_thing_of_the_past_says_private_investigator?nlid=1&source=NLT_AM; Steve Rambam, *Privacy Is Dead—Get Over It*, GOOGLE VIDEOS (Jan. 28, 2011), http://video.google.com/videoplay?docid=-383709537384528624. Steve Rambam is the controversial founder and CEO of Pallorium, Inc., a private investigations firm, and owner of PallTech, an investigative database service with more than 25 billion records on United States citizens and businesses. Mitchell, *supra*.

2. Don Butler, *Big Brother Is Watching, More Than Ever Before*, THE VANCOUVER SUN, Feb. 3, 2009, at F8; Don Butler, *Are We Addicted to Being Watched?*, OTTAWA CITIZEN (Jan. 31, 2009), http://www2.canada.com/ottawacitizen/news/observer/story.html?id=ade6d795-4e7a-4ede-9fc1-f7bf929849c8.

3. One study reported that eighty-nine percent of Internet users have voluntarily revealed personal information online. Carrie-Ann Skinner, *Majority of Web Users Share Personal Data Online*, COMPUTERWORLD (Aug. 12, 2008, 12:00 PM), http://www.computerworld.com/s/article/9112302/Majority_of_Web_users_share_personal_data_online?taxonomyId=84&intsrc=kc_feat&taxonomyName=privacy.

4. *Top 20 Countries with the Highest Number of Internet Users*, INTERNET WORLD STATS, http://www.internetworldstats.com/top20.htm (last visited Feb. 15, 2011).

5. Seventy-one percent of adult Internet users shop online. *Generational Differences in Online Activities*, PEW INTERNET (Jan. 28, 2009), http://www.pewinternet.org/Infographics/Generational-differences-in-online-activities.aspx.

6. Sixty-eight percent of adult Internet users make travel reservations online. *Id.*

7. Fifty-five percent of adult Internet users bank online. *Id.*

8. Fifty-nine percent of adult Internet users visit government websites. *Id.*

9. Thirty-five percent of adult Internet users use social networking sites. *Id.*

names, home addresses, telephone numbers, dates of birth, credit card numbers, and a plethora of other "personally identifying information."[10] We seemingly trust that the websites to whom we give this information will handle the information responsibly and refrain from disclosing the information in any way we do not intend or that may do us harm. Yet those sites use our personally identifying information to predict our behavior, to deliver advertising based upon the interests and habits gleaned from that information, and, ultimately, to generate revenue.[11]

This article is intended to be a discussion of the legal aspects of Internet *privacy*,[12] the right and ability to control what information one reveals about oneself over the Internet, who can access that information, and how that information can be used. It is not intended to be a discussion of Internet *security*, which is a related topic but focuses on the way that information (including, but not limited to, personally identifying information) is protected against unauthorized access, use, disclosure, and loss or destruction.[13] We presume, as many others have concluded,[14] that Internet privacy is important and trouble ourselves only with the mechanism by which our Internet privacy may be enhanced.

10. Generally speaking, "personally identifying information" or "PII" is information which can be used to identify an individual, such as that person's name, address, email address, credit card number, or Social Security number. *See generally Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles*: *Hearing Before the Subcomm. on Telecomms., Trade, and Consumer Prot. of the H. Comm. on Commerce*, 106th Cong. 2 (2000) [hereinafter *Internet Privacy Hearings*] (statement of Linda D. Koontz, Director, Information Management Issues), *available at* http://www.gao.gov/new.items/d01113t.pdf (discussing a federal study regarding the PII that different federal websites obtain).

11. *See, e.g.*, *Facebook Sponsored Stories: Letting Companies Use User Content to Advertise*, L.A. TIMES TECHNOLOGY BLOG (Jan. 25, 2011, 5:40 PM), http://latimesblogs.latimes.com/technology/2011/01/facebook-sponsored-stories-allow-companies-use-status-updates-places-check-ins-to-advertise.html (discussing a new Facebook feature that will allow companies to take user content and turn it into an advertisement).

12. "'Information privacy' is the term theorists use to discuss the privacy implications of the collection, use, and disclosure of personal information." Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1413 n.118 (2001) (discussing privacy problems with databases).

13. *Internet Privacy Hearings*, *supra* note 10, at 6.

14. *See, e.g.*, Rachel K. Zimmerman, Note, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century*, 4 N.Y.U. J. LEGIS. & PUB. POL'Y 439 (2000) (discussing the threats the Internet poses to personal privacy and proposing a multi-faceted solution that includes both constitutional and statutory remedies).

Part II of this article describes the current federal regulatory and statutory scheme devoted to Internet privacy and addresses the legislative actions taken by a few states to address the issue.[15] Part III describes the Internet privacy standards articulated by a few foreign nations—the European Union, United Kingdom, and Canada.[16] Part IV describes notable attempts to privately enforce Internet privacy rights through litigation.[17] Finally, Part V makes a case for the enactment of omnibus federal Internet privacy legislation, which leverages private enforcement to enhance the Internet privacy of all U.S. citizens.[18]

II. CURRENT PROTECTIONS

A. The Federal Trade Commission

The Federal Trade Commission (FTC) is the primary governing body tasked with the responsibility of protecting the privacy of information gathered online. The FTC derives its authority from section 5 of the Federal Trade Commission Act (FTCA), which broadly prohibits unfair or deceptive acts or practices in the marketplace.[19] Under the FTCA, the FTC has the power to extend online data protection by rulemaking.[20] However, rather than promulgate privacy rules, the FTC largely subscribes to a policy of "self-regulation" for most industry sectors.[21] With the

15. *See infra* Part II.
16. *See infra* Part III.
17. *See infra* Part IV.
18. *See infra* Part V.
19. 15 U.S.C. §§ 41–58 (2006). Specifically, section 5(a) provides that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." *Id.* § 45(a)(1).
20. *Id.* § 57a(a) ("[T]he Commission may prescribe . . . rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce (within the meaning of [section 45(a)(1) of this title] . . . .").
21. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS i–ii (June 1998) [hereinafter PRIVACY ONLINE], *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf ("The Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace and has held a series of workshops and hearings on such issues. Throughout, the Commission's goal has been to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online."); *see also* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 6 (July 1999) [hereinafter SELF-REGULATION AND PRIVACY ONLINE], *available at* http://www.ftc.gov/os/1999/07/privacy99.pdf (discussing the state of online privacy self-regulation). The Federal Trade Commission (FTC) has consistently stated that "self-regulation is the least intrusive and most efficient means to ensure

exception of financial services companies, health care providers, and web businesses that target children, the FTC permits the vast majority of businesses to establish their own privacy standards.[22] Accordingly, the FTC is only empowered to bring an enforcement action against a company if it makes false representations in its privacy policies that amount to "unfair or deceptive trade practices."[23] As a result, the FTC is constrained in its power to impact privacy protection in a meaningful way.

1. A Historical Look at the FTC's Approach to Internet Privacy

The FTC has endorsed two privacy models in the past fifteen years.[24] Starting in the mid-1990s, the FTC approached privacy policies, practices, and self-regulatory principles through the lens of fair information practices.[25] The FTC adopted, as the hallmarks of its self-regulation standards, the core principles of fair information practices, namely Notice, Choice, Access, and Security.[26] Of the four principles, the FTC placed the greatest emphasis on the principle of notice and successfully advocated for privacy policies as an industry norm.[27] During this time, the FTC,

fair information practices, given the rapidly evolving nature of the Internet and computer technology." *Id.*

22. CHARLES H. KENNEDY, THE BUSINESS PRIVACY LAW HANDBOOK 3 (2008) ("[O]nline businesses in the United States are free to collect, use, and disclose personal information in any way they choose, so long as those practices do not violate commitments they have made to parties providing that information. Put another way, American businesses generally are subject only to the online personal information rules they impose on themselves.").

23. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2114 (2004) ("[T]he agency is powerless—absent a specific statutory grant of authority—to regulate the collection of personal data by companies that either make no promises about their privacy practices or tell individuals that they will engage in unrestricted use and transfer of their personal data.").

24. Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at Proskauer on Privacy 1 (Oct. 19, 2010), *available at* http://www.ftc.gov/speeches/brill/101019proskauerspeech.pdf.

25. *Id.*

26. PRIVACY ONLINE, *supra* note 21, at 7; *see also Internet Privacy Hearings*, *supra* note 10, at 2 (defining the four core principles: notice means that "[d]ata collectors must disclose their information practices before collecting personal information from consumers;" choice means that "[c]onsumers must be given options with respect to whether and how personal information" is collected and how it may be used; access means that "[c]onsumers should be able to view and contest the accuracy and completeness of information collected about them;" and security means "[d]ata collectors must take reasonable steps to ensure that information collected from consumers is . . . secure from unauthorized use.").

27. HAROLD F. TIPTON & MICKI KRAUSE, INFORMATION SECURITY MANAGEMENT

the states, and consumer advocate groups appealed to Congress to codify the fair information practices into law, but Congress refused to enact any such federal omnibus scheme.[28]

As the market progressed, the burden fell on the consumer to navigate incomprehensible privacy policies.[29] In response, the FTC shifted its approach in the early part of the decade to a "harm-based" model designed to prevent tangible harm to consumers, such as harm from security breaches and harmful uses of information that cause economic injury.[30] The FTC targeted identity theft, spam, spyware, and children's privacy as its primary privacy initiatives.[31] As a result, the FTC focused its limited resources on security enforcement actions to address tangible harms to consumers, rather than privacy enforcement actions. In the past decade, the FTC has prosecuted twenty-five security enforcement actions and only four privacy enforcement actions.[32]

2. The FTC's Privacy Enforcement Actions

The FTC has broad discretion with regard to the enforcement actions it brings, yet it is limited by its statutory authority and financial resources.[33] Ironically, as the FTC's enforcement actions

HANDBOOK 2731 (6th ed. 2007) (noting that "almost all the top 100 commercial sites now post privacy policies" (citation omitted)).

28. Brill, *supra* note 24, at 2.

29. David Vladeck, Dir., Fed. Trade Comm'n Bureau of Consumer Prot., The Role of the FTC in Consumer Privacy Protection, Remarks Before the International Association of Privacy Professionals 9 (Dec. 8, 2009), *available at* http://www.ftc.gov/speeches/vladeck/091208iapp.pdf; *see also* Jon Leibowitz, Comm'r, Fed. Trade Comm'n, Concurring Statement Regarding FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising 3 n.2 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf ("A study of the privacy policies of Fortune 500 companies found that they were essentially incomprehensible for the majority of Internet users. Only one percent of the privacy policies were understandable for those with a high school education or less (like most teens and many consumers). Thirty percent of the privacy policies required a post-graduate education to be fully understood." (citing FELICIA WILLIAMS, INTERNET PRIVACY POLICIES: A COMPOSITE INDEX FOR MEASURING COMPLIANCE TO THE FAIR INFORMATION PRINCIPLES 17, 18 tbl.2 (2006), *available at* http://www.ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf)).

30. Brill, *supra* note 24, at 2; Vladeck, *supra* note 29, at 3.

31. Brill, *supra* note 24, at 2.

32. *See Privacy Initiatives*, FED. TRADE COMM'N, http://www.ftc.gov/privacy/privacyinitiatives/promises_press.html (last visited Feb. 15, 2011) (listing various press releases detailing prosecution of security and privacy enforcement actions by the FTC) (accessed by searching for the website at http://web.archive.org).

33. Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2056 (2000) ("[I]n principle, [the FTC] could bring enforcement

demonstrate, a company that has a privacy policy is subject to an FTC privacy enforcement action, whereas a company without a policy would not be.[34]

In 1998, the FTC brought its first Internet privacy enforcement action against GeoCities, one of the most popular sites on the Internet at the time.[35] The FTC alleged that GeoCities misrepresented the purpose for which it was collecting personally identifying information from children and adults.[36] Through its consumer registration process on its site, GeoCities created a database with email and postal addresses, member interest areas, income, education, gender, marital status, and occupation.[37] According to the FTC, GeoCities disclosed personally identifying information to third-party advertisers for targeted advertising.[38] The enforcement action resulted in a settlement which, most notably, required GeoCities to post on its site a clear and prominent privacy notice that disclosed to consumers the type of information it collected, the purpose of collecting that information, to whom it would disclose that information, and how consumers could access and remove their personal information. GeoCities was also required to obtain parental consent before collecting information from children twelve years old and under,[39] which was a prelude to the forthcoming Child Online Privacy Protection Act.

actions against websites merely on the basis of 'unfair' practices."). However, Hetcher contends that the FTC is prevented from doing so for political and practical reasons. *Id.* Practically, there are too many websites that are in violation of the FTC's fair information principles. *Id.* Politically, the approach in Washington has been towards "governmental non-interference with the Internet." *Id.*

34. *Id.* at 2056–58 ("The Agency has never brought an enforcement action against a website merely for 'unfair' trade practices."). However, Hetcher contends that once the website publishes a privacy policy, the FTC has jurisdiction to bring an enforcement action. *Id.* ("Once websites make explicit statements on their websites regarding their informational practices, they are then in a position in which they must either live up to those promises or open themselves up to the charge of engaging in deceptive trade practices.").

35. *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case,* FED. TRADE COMM'N (Aug. 13, 1998), http://www.ftc.gov/opa/1998/08/geocitie.shtm.

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

Similarly, in 2000, the FTC filed an enforcement action against ReverseAuction, an online auction site competitive with eBay.[40] The FTC alleged that ReverseAuction registered with eBay and agreed to eBay's User Agreement and Privacy Policy to market and promote its new site.[41] ReverseAuction subsequently harvested eBay users' personally identifying information to send users unsolicited messages promoting its own online auction site in an attempt to divert users away from eBay.[42] As part of the settlement, ReverseAuction was required to provide a privacy/notice policy on its website, refrain from using personally identifying information of eBay users who had not registered with ReverseAuction, and to create a process for consumers to cancel registration and have their personally identifying information deleted from ReverseAuction's database.[43] In the wake of the settlement, the Chairman of the FTC at the time stated:

> Confidence that privacy will be protected is an important element in consumers' decisions where to shop on the Internet. Self-regulatory efforts by e-businesses to protect their customers' privacy should be encouraged. But beyond self-regulation, those who violate consumers' privacy should be promptly called to task. Consumers should have confidence that their privacy choices will be protected.[44]

Despite the FTC's promises to improve Internet privacy protection, it continued to prosecute Internet security cases at a higher rate than privacy cases.[45]

In 2004, the FTC brought an enforcement action against Gateway Learning Corporation (Gateway), the company that markets and sells the "Hooked on Phonics" brand, for making

40. *Online Auction Site Settles FTC Privacy Charges*, FED. TRADE COMM'N (Jan. 6, 2000), http://www.ftc.gov/opa/2000/01/reverse4.shtm.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*; *see also* Timothy J. Muris, Chairman, Fed. Trade Comm'n, Remarks at The Privacy 2001 Conference (Oct. 4, 2001), *available at* http://www.ftc.gov/speeches/muris/privisp1002.shtm. The subsequent chairman similarly announced plans to increase resources dedicated to privacy protection by fifty percent. *Id.* ("We will enforce current laws vigorously, using more of the FTC's resources. We will stop those practices that are most harmful to consumers. We will use our full arsenal of tools . . . to pursue our strong pro-privacy agenda addressing real privacy concerns.").

45. *See Privacy Initiatives, supra* note 32 (listing a greater number of security cases than privacy cases).

material changes to its privacy policy without notifying consumers.[46] The FTC contended that Gateway rented consumers' personal information to third-party advertisers, contrary to explicit promises made in its initial privacy policy.[47] The FTC alleged that Gateway subsequently changed its privacy policy to allow for such disclosures to third-party advertisers, but continued to rent information collected under the initial policy without notifying consumers of the change.[48] The settlement provided, in part, that Gateway was prohibited from sharing any personal information collected from consumers under its initial privacy policy, unless it obtained affirmative "opt-in" consent from consumers.[49] The settlement also required Gateway to relinquish the $4,608 it earned from renting consumers' information, which it paid to the Treasury rather than to consumers.[50] This case was the first FTC enforcement action against a company for making material changes to its privacy policy without notifying consumers,[51] sending a signal to companies that they are obligated to honor statements made in their privacy policies.[52] However, some critics argue that the settlement was indicative of the FTC's weak enforcement ability, as evidenced by the paltry fine and Gateway's non-admission of liability.[53]

In a similar case, the FTC brought an enforcement action against a company for renting consumers' personal information to marketers in direct contravention to the privacy policies of the

46. *Gateway Learning Settles FTC Privacy Charges*, FED. TRADE COMM'N (Jul. 7, 2004), http://www.ftc.gov/opa/2004/07/gateway.shtm.

47. *Id.*

48. *Id.*

49. *Id.*

50. *Id.*

51. Bill Grabarek, *Gateway Learning Settles Privacy Charges*, DIRECT MAG. (Aug. 1, 2004), http://directmag.com/mag/marketing_gateway_learning_settles. According to Jessica Rich, an assistant director at the FTC at the time of the case, "[t]his is the first FTC case to allege deceptive and unfair practices in connection with a company's material change to its privacy policy." *Id.*

52. FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 11–12 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf. This case became the basis for one of the four governing principles of the FTC's self-regulatory guide for behavioral marketing: "before a company uses behavioral data in a manner that is materially different from promises made when the company collected the data, it should obtain affirmative express consent from the consumer." *Id.*

53. Adam G. Todd, *Painting a Moving Train: Adding "Postmodern" to the Taxonomy of Law*, 40 U. TOL. L. REV. 105, 139 (2008) ("The FTC's rather weak enforcement ability is illustrated by the consent decree that the FTC entered into with Gateway . . . .").

merchants with whom the company partnered.[54] The FTC brought the case against Vision I Properties, LLC, doing business as CartManager International, a company that provides shopping cart software and related services to thousands of online merchants.[55] CartManager collected and rented the personal information, including the name, address, phone number, email address, credit card number, and buying information, of nearly one million consumers who shopped at merchant sites.[56] The FTC alleged that CartManager failed to adequately inform consumers and merchants that it collected and rented this information and that such actions were contrary to many of the merchants' privacy policies.[57] As a result of this case, companies and service providers are now obligated to sync their individual privacy policies to avoid liability for any discrepancies.[58]

In a recent case, the FTC pursued an enforcement action against ControlScan, a company that verifies the privacy security of online retailers.[59] ControlScan acted as an independent auditor of merchant websites and placed seals on the sites to provide consumers with an indication of the level of the sites' security and privacy controls.[60] The FTC charged that ControlScan misled consumers about how often it monitored sites and the steps it took to verify the sites' security and privacy controls.[61] The settlement barred ControlScan from engaging in its certification practice and ordered them to pay $750,000, which was reduced to $102,000 due to the company's inability to pay the larger sum.[62]

54. *Internet Service Provider Settles FTC Privacy Charges*, FED. TRADE COMM'N (Mar. 10, 2005), http://www.ftc.gov/opa/2005/03/cartmanager.shtm.

55. *Id.* CartManager is the site that manages the "shopping cart" and "check out" pages of online merchants. *Id.*

56. *Id.*

57. *Id.*

58. *Id.* (quoting Lydia Parnes, Acting Director of the FTC's Bureau of Consumer Protection, as saying that "[c]ompanies and service providers must make sure that their privacy policies are in sync . . . . A service provider cannot secretly collect and rent consumers' personal information, contrary to a merchant's privacy policy. At the same time, merchants have an obligation to know what their service providers are doing with consumers' personal information").

59. *Online Privacy and Security Certification Service Settles FTC Charges*, FED. TRADE COMM'N (Feb. 25, 2010), http://www.ftc.gov/opa/2010/02/controlscan.shtm.

60. *Id.*

61. *Id.*

62. *Id.*

3. The Future of the FTC's Involvement

The FTC will continue to support industry self-regulation rather than government-imposed regulation to keep pace with the dynamic online marketplace.[63] On December 1, 2010, after a series of public roundtables and comment periods, the FTC issued a report that details its new approach to privacy.[64] The report attempts to balance the privacy interest of consumers while encouraging industry innovation[65] by addressing a number of key issues:

> •the collection and use of consumer information—both online and offline—is ubiquitous, and far more extensive than many consumers know.
>
> •consumers lack the understanding and ability in today's environment to make truly informed choices about the collection and use of their data.
>
> •even in today's environment of ubiquitous social networking, privacy is important to consumers.
>
> •the collection and use of consumer information provides significant benefits [to consumers, including] personalized advertising and other services, and, importantly, it underwrites so much of the free content available to consumers online.
>
> •and . . . the distinction between [personally identifying information (PII)] and non-PII is blurring.66

In response to these concerns, the report explores three self-regulatory proposals: privacy by design, transparency, and consumer choice.[67] Despite the FTC's continued affirmation of

63. *See* Brill, *supra* note 24, at 5.

64. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

65. Jon Leibowitz, Chairman, Fed. Trade Comm'n, Remarks Regarding the Preliminary FTC Staff Privacy Report 1 (Dec. 1, 2010) [hereinafter Leibowitz Remarks], *available at* http://www.ftc.gov/speeches/leibowitz/101201privacyreportremarks.pdf ("The FTC wants to help ensure . . . that the growing, changing, thriving information marketplace is built on a framework that promotes privacy, transparency, business innovation and consumer choice.").

66. *See* Brill, *supra* note 24, at 3–4.

67. *Id.* at 4 (explaining that "privacy by design" means building security and privacy "into commercial technologies and information practices from the outset"). Brill also discussed the need for transparency through better privacy policies "that are shorter, more comprehensible, and more consistent." *Id.* Lastly, Brill addressed the need for increased consumer choice through privacy notices that focus on the "unexpected" use of consumer data and a "centralized 'Do Not

self-regulation to protect online privacy, it recognizes its limitations, particularly in the areas of behavioral advertising and teen privacy.[68]

B. Federal Statutes

The United States lacks comprehensive national privacy legislation. The Children's Online Privacy Protection Act (COPPA) and the Electronic Communications Privacy Act (ECPA) are two of the primary federal statutes that provide remedies to individual online consumers for privacy infringement.

1. The Children's Online Privacy Protection Act

Congress enacted COPPA in 1998[69] after the FTC reported widespread abuse among operators of websites targeting children in the collection and use of personally identifying information.[70] In the following year, the FTC issued its Children's Online Privacy Protection Rule (the Rule), which became effective on April 21, 2000.[71] The FTC report that prompted Congress to enact the law revealed that website operators were easily able to engage children directly, without parental supervision, to obtain personal information for marketing purposes.[72]

The primary goal of COPPA is to give parents control over what type of information is collected from their children online and how that information may be used.[73] COPPA is significant because it is the first federal law to impose substantial obligations on website operators. The Rule applies to operators of commercial

Track' mechanism that would give consumers some control over the extent to which their online behavior is tracked." *Id.* *See also* Leibowitz Remarks, *supra* note 65, at 6 ("The most practical method would likely involve the placement of a persistent setting on the consumer's browser, signaling the consumer's choices about whether or not to be tracked.").

68. *See* Brill, *supra* note 24, at 6.

69. 15 U.S.C. §§ 6501–6508 (2006).

70. JANE K. WINN & BENJAMIN WRIGHT, LAW OF ELECTRONIC COMMERCE 14–36, 37 (4th ed. Supp. 2009).

71. 16 C.F.R. §§ 312.1–312.12 (2010).

72. WINN & WRIGHT, *supra* note 70, at 14–37 ("[A]ccording to the FTC data, 97 percent of parents whose children used the Internet believed that Web sites should not sell or rent personal information relating to children, and 72 percent objected to a Web site's requesting a child's name and address when the child registers at the site, even if that information is only used internally.").

73. *Frequently Asked Questions About the Children's Online Privacy Protection Rule*, FED. TRADE COMM'N (Oct. 7, 2008), http://www.ftc.gov/privacy/coppafaqs.shtm.

websites and online services directed to children under thirteen years of age that collect personal information,[74] operators of general audience sites that knowingly collect personal information from children under thirteen years of age, and operators of general audience sites that have a separate children's area and that collects personal information from children under thirteen years of age.[75] Operators covered by COPPA and the Rule must:

- post a privacy policy on the homepage of the website and link to the privacy policy on every page where personal information is collected;[76]
- provide notice about the site's information collection practices to parents[77] and obtain "verifiable parental consent"[78] before collecting personal information from children;[79]
- give parents a choice as to whether their child's personal information will be disclosed to third parties;[80]

74. 15 U.S.C. § 6501(8) (defining personal information as "individually identifiable information about an individual collected online, including . . .(A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph").

75. 15 U.S.C. § 6502; *see also Children's Online Privacy, BCP Business Center*, FED. TRADE COMM'N, http://www.ftc.gov/privacy/privacyinitiatives/childrens.html (last visited Mar. 14, 2011) (providing legal resources that pertain to children's online privacy).

76. 16 C.F.R. § 312.3(a).

77. DONALD S. CLARK, SECRETARY, FED. TRADE COMM'N, CHILDREN'S ONLINE PRIVACY PROTECTION RULE: FINAL RULE AMENDMENT 9, http://www.ftc.gov/os/2005/04/050420coppafinalrule.pdf (last visited Mar. 14, 2011) ("The Rule . . . require[s] that operators make certain third-party disclosures to the public [including] provid[ing] parents with notice of their information practices.").

78. 16 C.F.R. § 312.5(b); *see also* CLARK, *supra* note 77, at 2 (explaining the Rule's requirement that operators make reasonable efforts in light of currently available technology to ensure that the operator has achieved "verifiable" consent). The FTC uses a sliding scale approach to determine what efforts are reasonable to balance the costs imposed by the method of obtaining parental consent and the risks associated with the intended uses of information. *Id.* at 2–6. A less rigorous means of verifiable consent will be required if the information is only to be used internally, while a more rigorous means will be required if the information is disclosed to a third party. *Id.* The sliding scale provision was originally set to expire on April 21, 2002, but was extended for an additional three years. *Id.* In 2005, the sliding scale provision was extended indefinitely. *Id.*

79. 16 C.F.R. § 312.3(b).

80. *See id.* § 312.6 (a)(2).

- provide parents access to their child's personal information and the opportunity to require the operator to delete the child's personal information and opt-out of future collection or use of the information;[81]
- not condition a child's participation in a game, contest or other activity on the child's disclosing more personal information than is reasonably necessary to participate in that activity;[82] and
- maintain the confidentiality, security, and integrity of personal information collected from children.[83]

The FTC is responsible for enforcement of the COPPA and the Rule through section 5 of the FTCA.[84] In 2000, the FTC filed its first COPPA enforcement action when it amended a complaint in an existing case against Toysmart.com (Toysmart).[85] Through its website, Toysmart collected detailed personal information, including names, email addresses, and ages of children under thirteen years of age without notifying parents or obtaining parental consent.[86] The settlement of that complaint required Toysmart to immediately delete or destroy all information collected in violation of COPPA.[87]

Since the Toysmart settlement, the FTC has pursued fifteen additional cases asserting violations of COPPA.[88] Historically, the civil penalties range from $10,000 to $1 million in more recent cases.[89] Yet, critics argue that the FTC has failed to timely act on complaints in recent years.[90] Furthermore, COPPA has failed to

81. *Id.*
82. *Id.* § 312.3(d).
83. *Id.* § 312.3(e).
84. 15 U.S.C. § 6505 (2006).
85. *FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, FED. TRADE COMM'N (July 21, 2000), http://www.ftc.gov/opa/2000/07/toysmart2.shtm.
86. *Id.*
87. *Id.*
88. *See Legal Resources: Privacy and Security: Children's Online Privacy, BCP Business Center*, FED. TRADE COMM'N, http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html (last visited Mar. 14, 2011).
89. *See, e.g., Sony BMG Music Settles Charges Its Music Fan Websites Violated the Children's Online Privacy Protection Act,* FED. TRADE COMM'N (Dec. 11, 2008), http://www.ftc.gov/opa/2008/12/sonymusic.shtm; *Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule*, FED. TRADE COMM'N (Sept. 7, 2006), http://www.ftc.gov/opa/2006/09/xanga.shtm (providing examples of recent cases with $1 million civil penalties).
90. *See An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act (COPPA): Hearing Before the S. Comm. on Commerce, Sci.,*

keep pace with emerging social networking services and the "extensive data collection of both the trivial and the intimate information that children . . . share" over the Internet.[91]

Most social network services, such as Facebook, MySpace, and Twitter, prohibit participation by children that are thirteen years of age or under, which makes them generally exempt from the requirements of COPPA.[92] However, consumer rights advocates argue that COPPA should be extended to cover adolescents between the ages of thirteen and eighteen, because of their active participation in social networking and digital media.[93] Critics argue that social networking sites are making it increasingly difficult to navigate privacy policies and privacy settings, leading adolescent consumers to reveal their personal information.[94] Furthermore, adolescents are more likely to be impulsive than adults and may be less likely to think about the consequences of disclosing personal information.[95] Accordingly, consumer protection groups are urging the FTC to consider expanding the application of the Rule.[96]

and Transp. and the S. Subcomm. on Consumer Prot., Prod. Safety, and Ins., 111th Cong. 40–47 (2010) [hereinafter *Children's Privacy Hearing*] (statement of Marc Rotenberg, Executive Director, EPIC), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111shrg66284/pdf/CHRG-111shrg66284.pdf (testifying about the limitations of COPPA and the need to expand privacy protections). Rotenberg claims that EPIC has filed complaints that have gone unanswered by the FTC, even as other federal entities have deemed the offending companies to be in violation of COPPA. *Id.*

91. *Id.* at 43.

92. *See, e.g.*, *id.* at 43 n.14 (showing Facebook as an example of a social network service that requires users to be at least thirteen years of age).

93. *Id.* at 45–46; *Children's Privacy Hearing*, *supra* note 90, at 38–40 (statement of Kathryn C. Montgomery, Ph.D., Professor, School of Communication, American University).

94. *Children's Privacy Hearing*, *supra* note 90, at 42 (statement of Marc Rotenberg) (testifying that EPIC raised this concern in a recently filed "friend of the court" brief regarding the business practices of Facebook); *Children's Privacy Hearing*, *supra* note 90, at 39 (statement of Kathryn C. Montgomery) ("Social networks have created privacy settings that create a false sense of security for teens. While young people may believe they are protecting their privacy, they remain totally unaware of the nature and extent of data collection, online profiling, and behavioral advertising that are becoming routine in these online communities.").

95. Brill, *supra* note 24, at 6 (noting that the consequences include identity theft, adverse consequences for college applications or employment opportunities, and can "open the door to bullies or predators").

96. *Children's Privacy Hearing*, *supra* note 90, at 40–47 (statement of Mark Rotenberg).

The flexibility of COPPA's basic framework permits the FTC to ensure that the law addresses new ways of collecting personal information from children.[97] Despite the FTC's typical practice of reviewing its regulatory rules every ten years, the FTC announced to Congress on April 29, 2010, that it will accelerate the review of the COPPA Rule to ensure that it adequately protects online privacy for children.[98] The public comment period[99] and Review and Roundtable have passed, but, as yet, there is no indication of whether the FTC will act to revise the Rule.

2. The Electronic Communications Privacy Act

Subject to certain exceptions, the ECPA (more specifically, the Stored Communications Act, 18 U.S.C. § 2701) prohibits a person or entity providing an "electronic communication service"[100] from "knowingly divulging[ing] to any person or entity the contents of a communication while in electronic storage by that service."[101] It also prohibits a person or entity providing a "remote computing service to the public"[102]0020from knowingly divulging the contents of certain communications.[103] As to both providers of electronic communication services and remote computing services, the statute prohibits the knowing disclosure of "a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity," but does not prohibit such disclosure to a private entity.[104]

97. *Children's Privacy Hearing, supra* note 90, at 5 (statement of Kathryn C. Montgomery).

98. *Children's Privacy Hearing, supra* note 90, at 12 (statement of Jessica Rich, Deputy Director, Bureau of Consumer Protection, Federal Trade Commission).

99. *See Public Comment(s) on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Act (COPPA) Through the Children's Online Privacy Protection Rule (COPPA Rule)*, FED. TRADE COMM'N, http://www.ftc.gov/os/comments/copparulerev2010/index.shtm (last visited Mar. 14, 2011) (compiling a list of the comments received during the public comment period).

100. An "electronic communications service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2006).

101. *Id.* § 2702(a)(1).

102. A "remote computing service" is "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711.

103. *Id.* § 2702(a)(2).

104. *Id.* § 2702(a)(3).

The statute provides for a private cause of action by persons "aggrieved by any violation" of the statute.[105] In such a case, the prevailing plaintiff may obtain "such preliminary and other equitable or declaratory relief as may be appropriate,"[106] an amount equal to his or her actual damages and any profits made by the defendant as a result of the violation of the ECPA, "but in no case . . . less than the sum of $1,000" and plaintiff's reasonable attorney's fees and costs.[107]

3. Pending Legislation

On May 4, 2010, former Representative Rick Boucher (D-Va.) and Representative Cliff Stearns (R-Fla.) released a draft of privacy legislation that would require greater disclosure of privacy practices and consumer consent to collect and use certain kinds of personal information.[108] The proposed legislation requires greater notice to consumers by obligating any company that collects personally identifying information about individuals to conspicuously display a clearly written, understandable privacy policy explaining how information is collected, used, and disclosed.[109] The bill also provides that most personally identifying information would be subject to "opt-out" rules, meaning companies would be permitted to collect information about individuals, unless the individual affirmatively opts out of that collection.[110]

However, the bill would require express "opt-in" consent to knowingly collect *sensitive* information about an individual, including information that relates to an individual's medical records, financial accounts, Social Security number, sexual orientation, government-issued identifiers, and precise geographic location information.[111] Companies would also be required to obtain affirmative permission to disclose information to

105. *Id.* § 2707(a).
106. *Id.* § 2707(b)(1).
107. *Id.* §§ 2707(b)(3)–(c).
108. *See* Best Practices Act, H.R. 5777, 111th Cong. (2010); *see also* Daniel Castro, *One Step Forward, Five Steps Back: An Analysis of the Draft Privacy Legislation,* INFO. TECH. & INNOVATION FOUND. (May 5, 2010), http://www.itif.org/files/2010-privacy-legislation.pdf (analyzing the draft legislation).
109. H.R. 5777 § 101; *see also* Press Release, U.S. Congressman Cliff Stearns, Stearns, Boucher Release Discussion Draft of Privacy Legislation (May 4, 2010), http://stearns.house.gov/News/DocumentSingle.aspx?DocumentID=183894 (providing an overview of the draft legislation).
110. H.R. 5777 § 103.
111. *Id.*

unaffiliated third parties, such as advertising networks that collect information about users, create profiles of the users, and target ads to individual users based on their profile.[112] Under the bill, the FTC would be the main enforcement agency and would be required to adopt rules to implement the measure.[113] States would also be tasked with enforcing the FTC's rules through state attorneys general or state consumer protection agencies.[114]

Nearly a decade has passed since Congress last considered consumer privacy legislation, and as a result, the proposed bill received a firestorm of criticism from both consumer groups and the industry.[115] Consumer groups criticize the bill for not going far enough to protect consumer privacy, while at the same time going too far in preempting state online privacy bills, including the state bills that provide for private rights of action.[116] On the other side of the debate, industry groups criticize the bill for being overly broad, arguing that the opt-in requirements inhibit the free-flow of services and content that is currently provided to consumers largely free of charge.[117]

Rick Boucher was defeated in the November 2, 2010 elections, which has led many to speculate on the future of the bill.[118] However, shortly after the election, Representative Joe Barton (R-Tex.), announced that privacy was a priority for the next Congress.[119] Representative Ed Markey (D-Mass.) also expressed support for increased federal oversight of Internet privacy.[120] Even

112. *Id.* § 104.
113. *Id.* § 602.
114. *Id.* § 603.
115. *See* Stephanie Clifford, *Consumer Groups Say Proposed Privacy Bill Is Flawed*, N.Y. TIMES (May 4, 2010), http://www.nytimes.com/2010/05/05/business/media/05adco.html?_r=1.
116. *See id;* Andy Greenberg, *New Web Ad Privacy Bill Riles All Sides*, FORBES.COM (May 4, 2010, 5:18 PM), http://www.forbes.com/2010/05/04/privacy-web-advertising-technology-bill.html.
117. *See The Best Practices Act, and a Discussion Draft of Reps. Boucher and Stearns to Require Notice to and Consent of an Individual Prior to the Collection and Disclosure of Certain Personal Information Relating to that Individual: Hearing on H.R. 5777 Before the Subcomm. on Commerce, Trade, and Consumer Prot. of the H. Energy and Commerce Comm.*, 111th Cong. 7–8 (2010) (testimony of Michael Zaneis, Vice President of Public Policy, Interactive Advertising Bureau), *available at* http://www.iab.net/media/file/Zaneis_ConsumerProtectionSubcommittee.pdf.
118. *See* Cecilia Kang, *Rep. Barton Pledges Push for Internet Privacy Oversight*, WASH. POST (Nov. 3, 2010), http://voices.washingtonpost.com/posttech/2010/11/rep_barton_pledges_push_for_in.html.
119. *Id.*
120. *Id.*

if Boucher's bill is ultimately dropped, some form of privacy legislation is likely in the future given the bi-partisan support for such comprehensive federal legislation.

C. State Statutes

1. California

California is a key player in Internet privacy legislation.[121] California has passed two innovative laws that are the first of their kind at the state and federal level.[122] While the California legislation impacts online privacy for all consumers, even those outside of California,[123] the legislation insufficiently addresses some of the major concerns highlighted by consumer interest groups.[124]

The California Online Privacy Protection Act of 2003 (OPPA) is the first of such ground-breaking statutes and requires commercial websites and online service operators who collect personally identifying information about California residents to provide those residents with a conspicuous electronic notice of posted privacy policies and to comply with those privacy promises.[125] Under the OPPA, privacy policies must contain certain information, including the following: personally identifying information collected, the categories of parties with whom this personally identifying information may be shared, and the process for notifying users of material changes to the applicable privacy policy.[126] Violation of this policy may result in civil penalties, private suits, and even action by the FTC.[127]

121. Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 88–89 (2007) (arguing for a new federal privacy law).

122. *See* CAL. BUS. & PROF. CODE § 22575 (West 2010); CAL. CIV. CODE § 1798.83 (West 2009); *see also* Ciocchetti, *supra* note 121, at 89 (discussing the California Online Privacy Protection Act (OPPA) of 2003).

123. *See* Ciocchetti, *supra* note 121, at 90, ("California law effectively acts as a national regulation in the sense that its reach extends beyond California's borders to require any person or company in the United States (and conceivably the world) that operates a Web site that collects [PII] from California consumers [to comply with the California law]." (citation omitted)). It can be difficult to distinguish between California consumers and consumers in other states, forcing many online businesses to post privacy policies to avoid any possible violations.

124. *See infra* notes 128–130 and accompanying text.

125. CAL. BUS. & PROF. CODE § 22575.

126. *Id.*

127. Ciocchetti, *supra* note 121, at 90 n.154.

While the OPPA notice requirement has broad-reaching effects for website operators across the nation with regard to the notice requirement, the legislation has caused little impact on actual data collection practices.[128] OPPA's privacy policy requirement is ineffective for a number of reasons.[129] Such policies are often difficult for the average user to understand and users rarely read them in practice because it would simply take too long to actually read all the privacy policies applicable to users' Internet activities.[130] Furthermore, privacy policies falsely "lead consumers to believe that their privacy is protected" when it may not be.[131] Finally, "there is not enough market differentiation" to inform consumer choice and most users have difficulty weighing the costs and benefits associated with sharing personally identifying information.[132]

Shortly after California enacted OPPA, the state legislature passed another trailblazing Internet privacy law, the "Shine the Light" law.[133] Under "Shine the Light," all non-financial businesses (including online businesses) with twenty or more employees that conduct business with California residents must disclose certain information-sharing practices to their consumers.[134] According to the law, businesses that have shared consumer information with third parties for marketing purposes within the last twelve months must provide instructions about how the consumer can make a disclosure request.[135] If a consumer makes a disclosure request, the business must supply the consumer with information about the disclosures made by the business, including the categories of personal information disclosed to third parties and the list of companies to which the consumer's personal information was disclosed for marketing purposes within the last calendar year.[136] If a business fails to respond to a disclosure request, the customer may collect a civil penalty of up to $500 or a civil penalty of up to

128. UC BERKELEY SCHOOL OF INFORMATION, KNOWPRIVACY 11 (June 1, 2009), *available at* http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.
129. *Id.* at 11–12.
130. *Id.* at 11.
131. *Id.*
132. *Id.* at 11–12.
133. *See* CAL. CIV. CODE § 1798.83 (West 2009). The law went into effect on January 1, 2005. *See id.* § 1798.83(i).
134. *Id.*
135. *Id.* §§ 1798.83(a), (b)(1).
136. *Id.* §§ 1798.83(a), (e)(6)(A).

$3,000 for willful or intentional failures.[137]

While the California law is one of the first attempts to address "list brokerage," which is "the compilation and sale of individuals' personal information," it also has limitations in protecting consumer privacy.[138] First, the disclosure may be over-inclusive, because the information in the disclosure does not have to be specific to the consumer who made the request.[139] Companies compile consumer information and "segment" that information into customer lists.[140] General disclosures of the segmented lists are permissible under the law.[141] Second, the purpose of the law is to provide information to consumers to assist them in making better choices about the companies with which they decide to do business. However, the law places the burden on consumers to make disclosure requests and to decipher the information obtained.[142] Third, the law is meant to shape consumer choice going forward, but it does not challenge or rectify disclosures to third-party advertisers that have already occurred.[143]

2. Connecticut

In 2008, the Connecticut legislature passed a privacy protection statute that requires any person who collects Social Security numbers in the course of business to create a privacy protection policy.[144] The privacy policy must be published or "publicly displayed," which means Internet companies must post their privacy policy on their web pages.[145] The policy must "(1) [p]rotect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers."[146]

137. *Id.* § 1798.84.
138. *California S.B. 27, "Shine the Light" Law*, EPIC.ORG., http://epic.org/privacy/profiling/sb27.html (last visited Nov. 10, 2010).
139. *Id.*
140. *Id.*
141. *See id.*
142. *See* CAL. CIV. CODE § 1798.83(a).
143. *See generally* CAL. CIV. CODE § 1798.83 (requiring disclosure only for personal information that has been disclosed within the immediately preceding calendar year).
144. CONN. GEN. STAT. ANN. § 42-471 (West 2010).
145. *Id.* § 42-471(b).
146. *Id.*

While this statute codifies certain notice standards, it is severely narrow in the information it protects and the businesses affected.[147] Furthermore, any violation of the statute results in a nominal civil penalty of $500 per violation to be deposited with the state treasury.[148] Such a remedy precludes a private right of action for the individual consumer and places enforcement responsibility on the Connecticut Attorney General. In 2009, Connecticut considered a bill that would "set limits on companies that track consumers across websites to deliver targeted advertisements based on their behavior."[149] However, the proposed legislation was rejected in favor of the more narrow Social Security law.

3. Minnesota

On March 1, 2003, Minnesota passed the Minnesota Internet Privacy Law,[150] the first state law of its kind in the country.[151] Minnesota's privacy law prohibits Internet service providers (ISPs) from disclosing certain personally identifying information concerning their customers without customer authorization.[152] "The request for authorization must reasonably describe the types of persons to whom personally identifiable information may be disclosed and the anticipated uses of the information."[153] A consumer who prevails in an action brought under the law may be entitled to a minimum of $500 or a maximum of the actual damages incurred, as well as costs and attorney's fees.[154] While Minnesota is leading the way in privacy legislation of this kind, the legislation is limited in its ability to protect consumers in a meaningful way. Much like the ECPA, the Minnesota law only regulates the information disclosure practices of ISPs, leaving private website operators largely unfettered.[155]

147. *See id.* §§ 42-471(b)–(c).
148. *See id.* § 42-471(e).
149. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 917 (2009) (citing H.B. 5765, Gen. Assem., Feb. Sess. (Conn. 2008)) (examining privacy statutes in the United States).
150. MINN. STAT. § 325M (2009).
151. Jordan M. Blanke, *Minnesota Passes the Nation's First Internet Privacy Law*, 29 RUTGERS COMPUTER & TECH. L.J. 405, 407 (2003) (examining Minnesota's internet privacy law).
152. MINN. STAT. §§ 325M.02–.04.
153. *Id.* § 325M.04, subdiv. 2.
154. *Id.* § 325M.07.
155. *See id.* § 325M.09 ("This chapter applies to Internet service providers in the provision of services to consumers in this state.").

4. Nebraska

In 2003, Nebraska amended its deceptive trade practices statute to prohibit companies from knowingly making false or misleading statements in their Internet privacy policies.[156] While this provision may provide a cause of action against businesses that fail to adhere to their Internet privacy policies, Nebraska law does not mandate that every business adopt and implement such a policy. In effect, this law may provide a disincentive for companies to adopt a privacy policy because doing so may only subject them to liability.[157] However, Nebraska law does provide a general "right to privacy" cause of action, which may provide protections against the misuse of personal information on the Internet.[158]

5. Nevada

Nevada joins Massachusetts and California as one of the more proactive and aggressive states in terms of its Internet privacy regulations. In January 2010, Nevada enacted a new law requiring all businesses to encrypt personally identifiable customer information, including Social Security numbers, driver's license numbers, and credit card or other account numbers.[159] Specifically, the law requires that any "data collector"[160] transferring any personal information through an electronic, non-voice transmission (other than fax) to encrypt the information to ensure

156. *See* NEB. REV. STAT. § 87-302(a)(14) (2007) ("A person engages in a deceptive trade practice when, in the course of his or her business, vocation, or occupation, he or she . . . [k]nowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public.").

157. Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 616 (2008) ("[T]he . . . Nebraska laws only mandate that companies tell the truth in their privacy policies—a practice that may only encourage companies to fail to post a privacy policy rather than face the scrutiny of the state law.").

158. *See, e.g.*, Shlien v. Bd. of Regents, Univ. of Neb., 640 N.W.2d 643, 646–47 (Neb. 2002) (noting that a student brought a right to privacy action against a university professor for wrongfully posting the student's paper on the Internet without authorization).

159. NEV. REV. STAT. ANN. §§ 603A.010–.215 (LexisNexis 2010).

160. "Data collector" is defined under the statute as "any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information." *Id.* § 603A.030.

its secure transmission.[161] A data collector is also prohibited from moving "any data storage device containing personal information beyond the logical or physical controls of the data collector . . . unless the data collector uses encryption to ensure the security of the information."[162] Not only does this law regulate resident businesses, but non-resident businesses with customers or operations in Nevada are subject to the requirements as well.[163]

The new law places additional constraints on website operators collecting any "payment card" information in connection with the sale of goods or services. Websites subject to this law must comply with the Payment Card Industry Data Security Standard (PCI DSS).[164] Furthermore, Nevada's comprehensive legislation includes a data breach notification law, which requires a data collector to disclose a security breach to the owner of the information if the data collector determines that personal information has been accessed by an unauthorized person.[165]

Nevada also subjects ISPs to misdemeanor penalties for unlawfully disclosing certain subscriber information, with the exception of a subscriber's email address, without the subscriber's informed, written consent.[166] Although the statute does not require a subscriber's written consent for ISPs to disclose the subscriber's email address, the subscriber may opt-out by providing written

161. *Id.* § 603A.215(2)(a).

162. *Id.* § 603A.215(2)(b). Because of the broad statutory definition of "storage device," this provision impacts the use of laptops, iPhones, Blackberrys, or any other electronic device capable of storing personal information. *See* Philip Gordon, *New Nevada Law Mandates Encryption of Sensitive HR Data*, WORKPLACE PRIVACY COUNSEL (June 15, 2009), http://privacyblog.littler.com/2009/06/articles/data-security/new-nevada-law-mandates-encryption-of-sensitive-hr-data.

163. *See* NEV. REV. STAT. ANN. § 603A.200(2)(a) (defining "business" as anyone doing business in the state of Nevada); Ben Worthen, *New Data Privacy Laws Set for Firms*, WALL ST. J., Oct. 16, 2008, at B1.

164. NEV. REV. STAT. ANN. § 603A.215(1); *see also* Robert V. Connelly, Jr., *Are Online Privacy Policies Required by Law?*, THE RVC BLOG (Oct. 25, 2010), http://www.rendervisionsconsulting.com/blog/are-online-privacy-policies-required-by-law (last visited Jan. 31, 2011) (analyzing federal and state laws to determine when online privacy policies are required by law). "The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data." *PCI Security Standard Documents*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/security_standards/documents.php (last visited Mar. 14, 2011).

165. NEV. REV. STAT. ANN. § 603A.220 (LexisNexis 2010).

166. NEV. REV. STAT. ANN. § 205.498 (LexisNexis 2006).

notice to the ISP to prevent such disclosures.[167]

6. New York

Pursuant to New York's Internet Security and Privacy Act, state agencies are prohibited from disclosing or collecting any personal information concerning a user through state agency websites.[168] The law also requires state agencies to provide users with access to their personal information and the opportunity to correct or amend such information.[169] Moreover, the law requires the state to create a model Internet privacy policy, which state agencies must adopt and publish on their websites.[170] Although these regulations apply only to state agencies and not to private businesses or ISPs, New York's deceptive trade practices statute could be used to require companies to comply with their Internet privacy policies.[171]

7. Pennsylvania

Like Nebraska, Pennsylvania law includes in its deceptive or fraudulent business practices statute a provision prohibiting a business from knowingly making "a false or misleading statement in a privacy policy, published on the Internet . . . regarding the use of personal information submitted by members of the public."[172] However, without a law mandating that each business adopt a privacy policy, Pennsylvania's deceptive business practices statute merely creates disincentive for risk-averse companies to publish privacy statements and risk liability under those statements.[173]

167. *Id.* § 205.498(1)(b); *see also* Ciocchetti, *supra* note 157, at 623 n.224 ("The Nevada law also requires ISPs to provide a privacy notice to customers concerning the requirements of this statute . . . .").

168. N.Y. STATE TECH. LAW § 204 (McKinney 2003).

169. *Id.* § 205.

170. *Id.* § 203.

171. *See* Ciocchetti, *supra* note 157, at 617 ("New York's deceptive practices and false advertising statute has been used to require companies to honor their privacy policy promises."); *see also* Anonymous v. CVS Corp., 728 N.Y.S.2d 333, 339–40 (2001) (analyzing plaintiff's deceptive practices claim against CVS for disclosing plaintiff's prescription information despite statements made on CVS's website expressing its commitment to keeping customer information confidential).

172. 18 PA. CONS. STAT. ANN. § 4107(a)(10) (West 2005).

173. *See* Ciocchetti, *supra* note 157, at 616 (noting that the Pennsylvania law may only discourage companies from posting privacy policies to avoid scrutiny).

In 2005, Pennsylvania enacted the Breach of Personal Information Notification Act.[174] The Act requires that any "entity that maintains, stores or manages computerized data that includes personal information" provide notice to any resident of Pennsylvania if the entity "reasonably believe[s]" that such personal information has been accessed by an unauthorized person.[175] Pennsylvania joins the overwhelming majority of states who have enacted similar data breach notification laws.[176] While notification statutes ensure that individuals can take the proper steps to remedy a breach of their personal information, such statutes fall short of providing a solution to prevent the security breach in the first place. Indeed, data breach notification laws have been characterized as laws that "deal with what happens after the horse leaves the barn."[177]

8. Utah

In 2004, Utah passed the Government Internet Information Privacy Act, aimed at regulating governmental entities' websites.[178] The Act prohibits a governmental entity from collecting "personally identifiable information" through its website unless the entity has taken "reasonable steps to ensure" that the governmental website contains a privacy policy.[179] The privacy policy must, *inter alia*, disclose a summary of how the personally identifiable information is used, the practices related to disclosure of such information, the procedures by which a user may view and correct his or her information, and "a general description of the security measures in place to protect a user's personally identifiable information from

174. 73 PA. CONS. STAT. ANN. § 2301 (West 2010).

175. *Id.* § 2303(a) ("An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.").

176. *State Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=13489 (last updated Oct. 12, 2010). Only four states, Alabama, Kentucky, New Mexico, and North Dakota, have failed to enact similar laws. *Id.*

177. *See* Worthen, *supra* note 163 (citation omitted) (noting that researchers at Carnegie Mellon University found that data breach notification laws only reduce identity theft by about 2 percent).

178. UTAH CODE ANN. §§ 63D-2-101 to -2-104 (LexisNexis 2008).

179. *Id.* §§ 63D-2-103(1) to -2-103(2).

unintended disclosure."[180] Personally identifiable information under the Act includes any information that identifies "a user by (i) name; (ii) account number; (iii) physical address; (iv) email address; (v) telephone number; (vi) Social Security number; (vii) credit card information; or (viii) bank account information."[181]

In addition, Utah enacted the Notice of Intent to Sell Nonpublic Personal Information Act, which requires all commercial entities to disclose to customers the types of nonpublic personal information that a business shares with or sells to a third party for compensation.[182] "'Nonpublic personal information' includes: (i) a person's Social Security number; (ii) information used to determine a person's credit worthiness including a person's: (A) income; or (B) employment history; (iii) the purchasing patterns of a person; or (iv) the personal preferences of a person."[183] The law closely follows California's law requiring businesses to disclose to consumers any personal information the business shares or sells to third parties for direct marketing purposes.[184] Although not directly targeted at Internet businesses, these two statutes directly affect Internet transactions, particularly in light of the expansive growth of e-commerce.

9. Virginia

In light of the Virginia legislature's findings that an "individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information . . . [and that t]he increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices," Virginia enacted the Government Data Collection and Dissemination Practices Act.[185] The Act sets forth several principles "to ensure safeguards for personal privacy," including a requirement that all information collected be used for the appropriate and relevant purpose for which it has been collected, mandating a "prescribed . . . procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant

180. *Id.* § 63D-2-103(2).
181. *Id.* § 63D-2-102(6)(a).
182. UTAH CODE ANN. §§ 13-37-101 to -37-203 (LexisNexis 2009).
183. *Id.* § 13-37-102(5)(b).
184. *See supra* note 134 and accompanying text (citing CAL. CIV. CODE § 1798.83 (West 2009)).
185. VA. CODE ANN. §§ 2.2-3800 to -3809 (West 2008).

information[,]" and requiring agencies to take proper measures to prevent the misuse of personal information.[186]

The Act also provides for an expansive definition of "personal information," which includes any information relating to a person's "education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record," or any information which "affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual . . . ."[187] Furthermore, the Virginia statute requires all public entities with an Internet website to "develop an Internet privacy policy and an Internet privacy policy statement that explains the policy" and conforms to the principles of the Act.[188]

10. Wisconsin

While Wisconsin has joined the forty-five states adopting data breach notification laws,[189] it has not, thus far, enacted any Internet-specific privacy laws. Although Wisconsin has created a Joint Committee on Information Policy and Technology tasked with reviewing "information management and technology systems, plans, practices and policies" to ensure "data security and integrity, [and] protection of the personal privacy of individuals who are subjects of databases of state and local governmental agencies,"[190] it nevertheless trails states such as California and Nevada in its Internet privacy legislation. Despite the lack of Internet-specific privacy laws, Wisconsin has enacted expansive industry-specific privacy legislation.[191] Such laws cover financial information privacy, government records privacy, and health information privacy.[192] Because these laws do not limit their application to personal information stored in a particular medium, they could be utilized

186. *Id.* § 2.2-3800(C).
187. *Id.* § 2.2-3801.
188. *Id.* § 2.2-3803(B).
189. *See* WIS. STAT. ANN. § 134.98 (West 2009) (requiring any Wisconsin business entity maintaining or licensing personal information to make reasonable efforts to provide notice to the subject of the personal information of any unauthorized access of the subject's personal information).
190. *Id.* § 13.58(5).
191. *See Wisconsin Privacy Laws*, OFFICE OF PRIVACY PROT., http://privacy.wi.gov/laws/wisconsin/pdf/wisconsin_general_privacy.pdf (last visited Mar. 14, 2011) (outlining industry-specific privacy laws under Wisconsin law).
192. *Id.*

to protect certain aspects of Internet privacy.[193]

III. COMPARABLE PROTECTIONS IN FOREIGN NATIONS

A. European Union

While the United States remains wedded to piecemeal legislation and sectoral regulation of Internet privacy, other leaders in the global community have responded to privacy concerns by enacting omnibus privacy laws. At the forefront is the European Union (EU), which adopted the EU Data Protection Directive on October 24, 1995.[194] Enacted as a comprehensive scheme to ensure data protection across all sectors and communication mediums, the Directive "instructs all Member States to enact laws that 'protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'"[195] It is this unambiguous declaration that the right to privacy is fundamental which creates the divergence in privacy policy between the United States and the EU. While the United States has balked at an outright proclamation that the right to privacy is fundamental and instead couches its privacy policies in the form of patchwork judicial decisions and legislative mandates, the EU has taken a more direct and comprehensive approach.[196]

193. *See, e.g.*, WIS. STAT. ANN. § 85.103 (allowing individuals applying for a driver's license or other identification card to request that the Wisconsin Department of Transportation maintain the confidentiality of the applicant's personal information); *Id.* § 100.54(2) (enabling a consumer to put a "security freeze" on his or her credit report to prevent a consumer reporting agency from releasing his or her credit report); *Id.* § 943.201 (prohibiting the unauthorized use of an individual's personal information); *Id.* § 943.41(3) (prohibiting credit card theft); *Id.* § 947.013(1v) (increasing the penalty for harassment if a person committing the harassment intentionally gains access to a record in electronic format that contains personally identifiable information regarding the victim).

194. Robert R. Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2784 (2002) (noting that the European Union (EU) Data Privacy Directive went into effect three years later on October 25, 1998).

195. *Id.*

196. *See* Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 668 (2002) ("The European Union['s] . . . Data Privacy Directive . . . created a global model of a rigorous legislative approach to privacy . . . in contrast to the U.S. 'mix of legislation, regulation, and self-regulation.'"); Chuan Sun, Note, *The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective*, 2 NW. J. TECH. & INTELL. PROP. 99, 104–05 (2003) (discussing the fundamental differences in EU and United States approaches to privacy policy).

The EU's Directive begins with two seemingly inapposite objectives: (1) the protection of an individual's right to privacy with respect to personal data; and (2) enabling the free flow of personal data.[197] To that end, the Directive requires that any entity collecting personal information must do so for "specified, explicit and legitimate purposes," and must collect information that is "adequate and relevant for the stated purpose, accurate and current, and maintained in personal identifiable form for only the amount of time needed to accomplish the stated purpose for collection."[198]

The most unique feature however is the Directive's "opt-in" provision. Pursuant to Article 7 of the Directive, Member States may process personal data if "the data subject has unambiguously given his consent."[199] This opt-in requirement stands in stark contrast to the general policy adopted by the United States, which permits the processing of personal data unless the individual opts out. For example, in the United States, an individual must register with the "do not call" registry in order to avoid telemarketers; whereas, citizens of the EU must affirmatively consent to being contacted by direct marketing services.[200] Thus, the United States default favors the dissemination and access of personal data while the EU's default gives the owner of the information control over its dissemination.

The Directive's reach however does not merely implicate the twenty-seven EU Member States. Article 25, one of the Directive's more controversial provisions, provides that Member States may only transfer personal data to non-EU Member States if those non-Member States provide "an adequate level of protection."[201] This

197. Council Directive 95/46, Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) Art. I (EC) [hereinafter EU Directive].

198. Jonathan P. Cody, Comment, *Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation?,* 48 CATH. U. L. REV. 1183, 1212–13 (1999) (citation omitted) (studying Internet privacy regulations).

199. EU Directive, *supra* note 197, Sec. II, Art. 7. A Member State may also process personal data in situations in which processing is necessary to comply with legal orders or contracts or in other narrow exceptions. *Id.*

200. *See* Seagrumn Smith, *Microsoft and the European Union Face Off Over Internet Privacy Concerns*, 2002 DUKE L. & TECH. REV. 14, http://www.law.duke.edu /journals/dltr/articles/2002dltr0014.html ("This opt-out versus opt-in debate reflects a major philosophical difference in how the EU and U.S. regard personal data privacy . . . .").

201. EU Directive, *supra* note 197, Art. 25.

far-reaching provision caught the attention of the Clinton administration, which began negotiations with the EU to establish a "Safe Harbor" framework that would ensure that the Directive did not interrupt data flow from the EU to the United States.[202] By July 2000, the U.S. Department of Commerce had successfully negotiated the agreement through the EU, which voted to approve the Safe Harbor principles despite objection from a majority of the European Parliament.[203] Although membership in the Safe Harbor is voluntary, companies that do certify with the U.S. Department of Commerce agree that they will comply with the Safe Harbor principles.[204] Participants in the Safe Harbor are assured that their privacy protections will be "deemed adequate" and in compliance with the Directive, thus ensuring that data flow from the EU to the United States continues uninterrupted.[205]

In an effort to supplement the EU Directive to address concerns of an increasingly electronic global environment, the European Commission (EC) adopted the Electronic Privacy Directive (e-Privacy Directive) in 2002.[206] The e-Privacy Directive retains the opt-in approach utilized by the original Directive by allowing "the use of automatic calling machines, faxes, or e-mail for purposes of direct marketing . . . only for those subscribers who have given their prior consent. In other words, the EU has adopted an opt-in approach to spam."[207] Furthermore, the e-Privacy Directive "prohibits companies from taking personal data from websites or finding the location of satellite-linked mobile telephone

202. Salbu, *supra* note 196, at 678.

203. *Id.* at 679–80 (noting that the European Parliament was skeptical of the Safe Harbor because it lacked an independent body capable of adjudicating violations).

204. *See* Schriver, *supra* note 194, at 2790–91 (enumerating the Safe Harbor principles, including the requirements that participating companies must give individuals the choice as to whether their personal information will be disclosed to third parties and that individuals must be given access to their personal information and the ability to correct or delete any inaccurate information).

205. *Id.* at 2789–90.

206. Directive 2002/58, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 207) (EC), *amended by* Directive 2009/136, 2009 O.J. (L 337) (EC).

207. George B. Delta & Jeffrey H. Matsuura, *European E-Commerce Initiatives*, *in* LAW OF THE INTERNET § 13.11, at 13-128 (2010); *see also* Ariella Mutchler, Note, *CAN-SPAM Versus the European Union E-Privacy Directive: Does Either Provide a Solution to the Problem of Spam?*, 43 SUFFOLK U. L. REV. 957, 972 ("[O]ne exception to the opt-in rule allows e-mail solicitation when the marketer obtains the e-mail address in the context of a sale of goods or services.").

users."[208]

In light of rapid advancements in technology and a generation immersed in social networking, the EC recently announced its intent to update the fifteen-year-old Directive, which will include revisions to the e-Privacy Directive.[209] The EC's overhaul will include efforts to make it easier for individuals to access, correct, and delete their personal information, and will implement a more stringent enforcement regime for privacy violations.[210]

B. United Kingdom

The United Kingdom (UK) enacted the Data Protection Act of 1998 to establish a framework to comply with the EU Directive.[211] The UK established the Information Commissioner's Office (ICO) as an independent authority assigned to be directly responsible for implementing the Data Protection Act.[212] The principles of the Act closely mirror those of the EU Directive, including requirements for fair and lawful processing of personal data and protections against electronic marketing messages (whether phone, fax, or email).[213]

Although the UK's Internet privacy laws are facially compliant with the EU Directive, the UK has been under intense scrutiny recently for failing to enforce these privacy principles. In September 2010, the EC referred the UK to the European Court of

208. Delta & Matsuura, *supra* note 207, at 13-128.

209. Drew Singer, *EU Calls for Stronger Internet Privacy Laws*, JURIST (Nov. 4, 2010, 10:36 AM), http://jurist.org/paperchase/2010/11/eu-calls-for-stronger-internet-privacy-laws.php.

210. EUROPEAN COMM'N, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION 2, (2010), *available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf ("[R]apid technological developments and globalisation have profoundly changed the world around us, and brought new challenges for the protection of personal data.").

211. *See* INFO. COMM'RS OFFICE, THE GUIDE TO DATA PROTECTION, http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Practical_application/THE_GUIDE_TO_DATA_PROTECTION.ashx.

212. *Id.* at 11–12.

213. *Id.* at 37–39; *see also* INFO. COMM'RS OFFICE, PRIVACY AND ELECTRONIC COMMUNICATIONS (EU DIRECTIVE) REGULATIONS 2003: WHEN AND HOW TO COMPLAIN ABOUT ELECTRONIC MARKETING MESSAGES, http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Introductory/PECR%20HOW%20TO%20COMPLAIN%20FINAL.ashx (stating that the Privacy and Electronic Communications Regulations of 2003 govern electronic marketing).

Justice for failing to comply with the EU regulations protecting the privacy of electronic communications.[214] Specifically, the EC found that UK privacy laws were not being properly implemented with respect to "Phorm," a system used by UK Internet service providers to "monitor user web-surfing habits and deliver personalized advertising without the user's consent."[215] The EC launched an infringement proceeding in April 2009 to address the UK's deficiencies, citing lax standards with regard to obtaining an individual's consent to have their personal information intercepted.[216] The EC requires that Member States have "procedures in place to ensure 'clear consent from the user that his or her private data is being used.'"[217] Although the UK put a halt to "Phorm" after the EC's infringement proceedings, the EC has nonetheless initiated legal proceedings in the European Court of Justice, calling for an overhaul of UK privacy laws.[218]

C. Canada

Although Canada generally shares the United States' affinity for self-regulation with respect to privacy law, it nevertheless has established its own omnibus regulation for the protection of personal data.[219] The Canadian Standards Association Model Code for the Protection of Personal Information (Model Code) was established in part to comply with the EU Directive.[220] The tenets of the Model Code have now been incorporated into the Personal

214. Megan McKee, *EU Suing UK over Internet Privacy*, JURIST (Sept. 30, 2010, 3:23 PM), http://jurist.org/paperchase/2010/09/eu-suing-uk-over-internet-privacy.php; Darren Waters, *EC Starts Legal Action over Phorm*, BBC NEWS (Apr. 14, 2009), http://news.bbc.co.uk/2/hi/technology/7998009.stm.

215. McKee, *supra* note 214.

216. *See* Waters, *supra* note 214 ("At the heart of the legal action by the EC is whether users have given their consent to have their data intercepted by the advertising system."); *Telecoms: Commission Launches Case Against UK over Privacy and Personal Data Protection*, EUROPA (Apr. 14, 2009), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&guiLanguage=en.

217. Waters, *supra* note 214.

218. McKee, *supra* note 214 ("Specifically, current UK law does not provide for an independent national authority to supervise the interception of some communications, it allows for communications to be received without fulfilling the EU definition of consent and it does not have a mechanism that ensures sanctions for unlawful unintentional interception, as required by EU law.").

219. Cody, *supra* note 198, at 1215–16.

220. *Id.* at 1216 ("[The Model Code] establishes ten practice principles that must be adopted as a whole by those who wish to participate . . . .").

Information Protection and Electronic Documents Act (PIPEDA).[221] Similar to the United States' Safe Harbor, participation in the PIPEDA is voluntary.[222] The PIPEDA standards very closely mirror the EU Directive principles, requiring that organizations collect, use, and disclose personal information by fair and lawful means, only with an individual's consent, and only for limited purposes.[223] Individuals also have the right to access their personal information and correct any inaccurate information.[224] PIPEDA also establishes recourse for individuals who believe their rights under the Act have been violated by allowing those individuals to file a complaint with the Privacy Commissioner.[225]

Recently, the Office of the Privacy Commissioner conducted a symposium on Internet Privacy Law in Canada, after which the Privacy Commissioner released a review of PIPEDA, including recommendations for updating and improving the Act.[226] While the Privacy Commissioner found that "PIPEDA is working reasonably well," it made nine recommendations to address certain deficiencies.[227] The recommendations included a call to improve anti-spam legislation.[228] Noting that Canada was the only G-8 nation without specific anti-spam legislation, the Privacy Commissioner warned that this deficiency was "undermining confidence in the Internet and even prompting some people to

221. *Principles in Summary: View Privacy Code*, CSA, http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code/article/principles-in-summary (last visited Mar. 14, 2011).

222. *See Introduction: View Privacy Code*, CSA, http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code/article/introduction (last visited Mar. 14, 2011) ("The [Privacy] Standards address[] two broad issues: the way organizations collect, use, disclose, and protect personal information; and the right of individuals to have access to personal information about themselves, and, if necessary, to have the information corrected.").

223. OFFICE OF THE PRIVACY COMM'R OF CAN., YOUR GUIDE TO PIPEDA, *available at* http://www.priv.gc.ca/information/02_05_d_08_e.pdf.

224. *Id.*

225. *See id.* "[U]nder certain circumstances, [aggrieved individuals may also] take [a] complaint to the Federal Court of Canada [if the Privacy Commissioner failed to resolve the dispute.]").

226. *The Privacy Commissioner of Canada's Position at the Conclusion of the Hearings on the Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)*, 8 PRIVACY & INFO. L. REP. 3, 4 (2007), *available at* http://www.priv.gc.ca/parl/2007/sub_070222_e.cfm (recommending changes to PIPEDA).

227. *Id.*

228. *Id.*

abandon electronic commerce."[229]

IV. PRIVATE ENFORCEMENT OF INTERNET PRIVACY PROTECTIONS THROUGH LITIGATION

A. *DoubleClick*

In 1999, Internet users brought a class action lawsuit against DoubleClick, the market leader in online advertising, in one of the first Internet privacy suits to be decided on the merits.[230] The users contended that DoubleClick placed "cookies"[231] on users' hard drives each time the users visited any one of the 11,000 sites for which DoubleClick provided targeted banner advertisements.[232]

Plaintiffs alleged that DoubleClick engaged in the intentional unauthorized access of electronic communication in violation of Title II of the ECPA when it tracked the communications between the plaintiffs and the affiliated websites through use of the cookies.[233] The court dismissed plaintiffs' claims, holding that the use of cookies fell within the exception for "conduct authorized . . . (2) by a user of that . . . service with respect to a communication of or intended for that user."[234] The court found that the affiliated websites were "users" within the meaning of the exemption and that as "users" the affiliated website consented to DoubleClick's access to the communications.[235] The court held that it was indisputable that the affiliated websites had consented or authorized DoubleClick to intercept communications, as evidenced by the commercial relationship to generate revenue from advertising.[236]

Similarly, the court dismissed plaintiffs' claim for violation of the Federal Wiretap Act.[237] Plaintiffs alleged that DoubleClick violated the act by intentionally "intercepting" electronic

229. *Id.*
230. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001.
231. The purpose of the cookies was to track users' communications with DoubleClick's affiliated websites to create profiles of the users for targeted advertising.
232. *DoubleClick*, 154 F. Supp. 2d at 502–03.
233. *Id.* at 510. "Communication" means the record of the particular pages visited by the plaintiffs at affiliated websites and the information the plaintiffs provide on those websites.
234. *Id.* at 507, 511; 18 U.S.C. § 2701(c)(2) (2006).
235. *DoubleClick*, 154 F. Supp. 2d at 508–09.
236. *See id.* at 511–14.
237. *Id.* at 519.

communications between plaintiffs and the affiliated websites.[238] However, the court held that DoubleClick fell within the statutory exception for consent by one of the parties to the communication, where the affiliated websites had consented to the "interception."[239]

The court also dismissed plaintiffs' Computer Fraud and Abuse Act (CFAA) claim for failure to plead the statutory threshold of $5,000 in damages for each individual class member.[240] The plaintiffs claimed damages resulting from the aggregate loss of their privacy, trespass to their personal property, and the misappropriation of confidential data by DoubleClick.[241] The court held that damages may only be aggregated across victims for a single act by the defendant, and that DoubleClick's actions are properly characterized as a series of single acts that individually affected plaintiffs.[242]

The court refused to exercise supplemental jurisdiction over the state law claims as a result of dismissing all of the federal claims.[243] The parties ultimately resolved the case in a highly publicized settlement prior to any appellate hearing.[244]

B. Intuit

One of the first Internet privacy lawsuits brought in federal court was a class action lawsuit filed in the United States District Court for the Central District of California against Intuit, a developer of financial and tax preparation software and operator of the website located at www.quicken.com.[245] In that case, plaintiffs alleged that a "cookie"[246] was placed on their computers while

238. *Id.* at 515.
239. *Id.* at 514–16.
240. *See id.* at 520–26.
241. *Id.* at 523.
242. *See id.* at 524–26.
243. *Id.* at 526.
244. *See DoubleClick Settles Online-Privacy Suits, Plans to Ensure Protections, Pay Legal Fees*, WALL ST. J., Apr. 1, 2002, at B8.
245. *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001).
246. As the court noted,

> [a] 'cookie' is an electronic file that online companies . . . implant upon computer users' hard drives when those users visit . . . Web sites such as Quicken[.]com . . . . Cookies generally perform many convenient and innocuous functions, such as keeping track of items Web site visitors may purchase . . . . [Cookies may] keep track of usernames and passwords to make it easier for people to access Web sites that require authentication . . . .

Id.

visiting www.quicken.com.[247] On this basis, plaintiffs alleged three claims under federal statutes and two supplemental state law claims.[248] Intuit filed a motion to dismiss for failure to state a claim upon which relief may be granted.[249]

Plaintiffs' first claim alleged a violation of § 2701 of the ECPA, which prohibits a person or entity from intentionally accessing "without authorization a facility through which an electronic communication service is provided; or . . . intentionally exceed[ing] an authorization to access that facility; and thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage . . . ."[250] Intuit argued that this claim should be dismissed because the plaintiffs failed to allege that defendant was a "third party to the communications at issue" and because the plaintiffs failed to sufficiently plead that the defendant "accessed an 'electronic communication while it [was] in electronic storage in' an electronic communication system."[251] The court denied the motion as to the ECPA claim, holding that the statute does not require a defendant to be a "third-party to the communications at issue" and that the "fact that Plaintiffs have alleged that certain electronic communications were intercepted in transit at one time does not preclude it from also alleging that other electronic communications were accessed while in electronic storage at another time."[252] However, the court granted the rest of Intuit's motion to dismiss, holding that plaintiffs failed to allege facts sufficient to support the remaining claims.[253]

C. Pharmatrak

In 2003, the United States Court of Appeals for the First Circuit considered a case brought against a number of pharmaceutical companies which raised "important questions about the scope of privacy protection afforded internet users under

247. *Id.*
248. *Id.*
249. *Id.* at 1273.
250. *Id.* at 1275.
251. *Id.* (footnote omitted). Apparently, Intuit abandoned an argument, asserted in its notice of motion but not in its opening brief, that its computers were not "communication service providers" under the statute. *Id.* at 1275 n.3.
252. *Id.* at 1275–77.
253. *Id.* at 1277–81.

the [ECPA] . . . ."[254] The pharmaceutical companies invited users to visit their websites for information about their drugs and to obtain rebates.[255] One company, Pharmatrak, sold a service to the pharmaceutical companies that accessed information about the users and collected certain information meant to permit the pharmaceutical companies to perform intra-industry comparisons of website traffic.[256] Most of the pharmaceutical companies clearly communicated that they did not want personal or identifying data about their website users to be collected, and they received assurance from Pharmatrak that such data would not be collected.[257] However, some users' personal and identifying data was later found on Pharmatrak's computers, leading the plaintiffs to file suit.[258]

The district court entered summary judgment for defendants on the basis that Pharmatrak's conduct was not an "interception" but fell within an exception to the ECPA which permits a third-party to obtain the contents of an electronic communication where one party to the communication consents.[259] The First Circuit addressed the issue on appeal.

In reversing and remanding the trial court's decision, the First Circuit noted that the ECPA amended the Federal Wiretap Act "by extending to data and electronic transmissions the same protection already afforded to oral and wire communications."[260] To this end, it provides a private right of action against a person who "intentionally intercepts,[261] endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . ."[262] The court also held that the ECPA's definition of the "contents" of an electronic communication encompassed the personally identifying information at issue.[263] The First Circuit found that the district

254. *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 12 (1st Cir. 2003).
255. *Id.*
256. *Id.*
257. *Id.*
258. *Id.*
259. *Id.* at 12–13 (applying 18 U.S.C. § 2511(2)(d) (2006)).
260. *Id.* at 18.
261. For the purposes of the statute, "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).
262. *Id.* § 2511(1)(a).
263. *Pharmatrak*, 329 F.3d at 18.

court had erred by not placing upon the defendants the burden of establishing the consent necessary to fall within the subject exception to liability under the ECPA.[264] Moreover, the court held that Pharmatrak's conduct constituted an "interception" within the meaning of the statute.[265]

D. Post-9/11 Airline Cases

Following the terrorist attacks of September 11, 2001, a number of governmental agencies commissioned studies geared toward improving security at airports, military bases, and other installations.[266] To conduct these studies, the government sought and obtained private information concerning airline passengers from a number of airlines.[267] Discovery of the airlines' disclosure of personal passenger information to governmental agencies triggered a flurry of litigation.[268]

1. Northwest Airlines

Without notifying its customers, Northwest provided the National Aeronautical and Space Administration (NASA) with the names, addresses, credit card numbers, identity of traveling companions, and travel itineraries (including hotel reservation and rental car information) of persons who had flown on Northwest between July and December 2001.[269] Discovery of this disclosure resulted in the filing of at least nine class action lawsuits—seven in Minnesota and one each in Tennessee and North Dakota.[270]

264. *See id.* at 19–20.
265. *See id.* at 22–23.
266. *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 304 (E.D.N.Y. 2005); *In re* Nw. Airlines Privacy Litig., No. Civ. 04-126(PAM/JSM), 2004 WL 1278459, at *1 (D. Minn. June 6, 2004; Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1197 (D.N.D. 2004).
267. *JetBlue*, 379 F. Supp.2d at 304; *Nw. Airlines*, 2004 WL 1278459, at *1; *Dyer*, 334 F. Supp. 2d at 1197.
268. *JetBlue*, 379 F. Supp.2d at 304; *Nw. Airlines,* 2004 WL 1278459, at *1; *Dyer*, 334 F. Supp. 2d at 1197.
269. *Nw. Airlines*, 2004 WL 1278459, at *1; *Dyer*, 334 F. Supp. 2d at 1197.
270. *Dyer,* 334 F. Supp. 2d at 1197.

a. Minnesota

In the Minnesota lawsuits, the plaintiffs alleged that Northwest's actions violated the ECPA, the Fair Credit Reporting Act (FCRA),[271] and Minnesota's Deceptive Trade Practices Act.[272] The plaintiffs also asserted certain common-law claims against Northwest, including invasion of privacy, trespass to property, negligent misrepresentation, breach of contract, and breach of express warranties.[273] The plaintiffs argued that the Northwest website contained a privacy policy which stated that Northwest would not share customers' information except as necessary to make customers' travel arrangements and that Northwest's disclosure of passenger information to NASA constituted a violation of that privacy policy.[274]

In response to the Minnesota cases, Northwest filed a motion to dismiss on the grounds that the plaintiffs failed to state any claims upon which relief could be granted.[275] Under then-existing federal standards for pleading, the United States District Court for the District of Minnesota construed the allegations in the plaintiffs' pleadings and made all reasonable inferences arising there from in favor of the non-moving party and considered each claim brought against Northwest.[276] The court dismissed each of the plaintiffs' claims.[277]

(1) ECPA Claim

With respect to their ECPA claim, the plaintiffs argued that Northwest's access to its own electronic communications service was limited by its privacy policy and that the disclosure of passenger information to NASA violated that policy and, therefore, constituted unauthorized access to the "facility through which an electronic communication service is provided" as prohibited by 18 U.S.C. § 2701(a)(1).[278] Plaintiffs also argued that the disclosure violated 18 U.S.C. § 2702, which prohibits "a person or entity providing an electronic communications service to the public . . .

271. 15 U.S.C. § 1681 (2006).
272. MINN. STAT. § 325D.44 (2010).
273. *Nw. Airlines*, 2004 WL 1278459, at *1.
274. *Id.*
275. *Id.*
276. *Id.*
277. *Id.* at *6.
278. *Id.* at *2.

[from] knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service."[279]

The court held that Northwest was not the provider of an "electronic communication service"[280] and, therefore, could not be held liable for violating § 2702 of the ECPA.[281] Moreover, the court held that plaintiffs failed to state a claim pursuant to § 2701 of the ECPA because that statute prohibited improper *access* to an electronic communications service provider of the information contained thereon, not improper *disclosure* of information.[282]

(2) FCRA Claim

In alleging their FCRA claim, the plaintiffs contended that Northwest or its electronic communications service provider was a "consumer reporting agency" and that the disclosure of passenger information to NASA constituted the furnishing of a "consumer report" to a third-party without the subject consumer's written consent, which is prohibited by the FCRA.[283] In finding that Northwest was not a "consumer reporting agency"[284] and that the passenger information disclosed to NASA was not a "consumer report"[285] under the FCRA, the court characterized the plaintiffs'

279. *Id.* (citation omitted).

280. *Id.* ("In fact, Northwest purchases its electronic communications service from a third party, Worldspan.").

281. *Id.*

282. *Id.* ("There is no dispute that Northwest obtained Plaintiffs' personal information properly, in the ordinary course of business. Plaintiffs' complaint is not with how Northwest obtained the information, but with how Northwest subsequently used the information. Because § 2701 does not speak to the use of the information, it does not apply and Plaintiffs' claims under § 2701 fail as a matter of law.").

283. 15 U.S.C. § 1681b(a)(2) (2006).

284. *Nw. Airlines*, 2004 WL 1278459, at *3 ("'[C]onsumer reporting agency' [means] any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." (citation omitted)).

285. *Id.* at *3 ("The term 'consumer report' means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purposes of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title." (citation omitted)).

FCRA claim as requiring "not liberal application of the statute, but wholesale disregard of the statute's purposes and definitions."[286]

(3) Deceptive Trade Practices and Negligent Misrepresentation Claims

Northwest successfully argued that plaintiffs' claims under the Deceptive Trade Practices Act (DTPA) and for negligent misrepresentation were preempted by the Airline Deregulation Act, 49 U.S.C. § 41713(b), which prohibits states from enacting or enforcing any law "related to[287] a price, route, or service of an air carrier."[288] In dismissing plaintiffs' DTPA and negligent misrepresentation claims, the district court noted that the preemption doctrine "bars state-imposed regulation of air carriers,"[289] including the regulation which might be imposed by state consumer protection laws.[290]

(4) Trespass Claim

Under Minnesota law, a plaintiff seeking to recover for trespass must demonstrate that: (1) she owned or possessed property; (2) that the defendant wrongfully took that property; and (3) that the plaintiff was damaged by the wrongful taking.[291] The court held that the passenger information disclosed to NASA was not the property of the plaintiffs but of Northwest and, since Northwest could not wrongfully take its own property, no trespass occurred.[292]

286. *Id.*

287. The Supreme Court determined that a law or claim "relates to" a price, route, or service of an air carrier where it has a "connection with or reference to" the airline's rates, routes, or services. Morales v. Trans World Airlines, Inc., 504 U.S. 374, 384 (1992).

288. 49 U.S.C. § 41713(b) (1994).

289. Am. Airlines, Inc. v. Wolens, 513 U.S. 219, 222 (1995).

290. *Nw. Airlines*, 2004 WL 1278459, at *4 (citing *Wolens*, 513 U.S. at 227–28).

291. *Id.* (citing H. Christiansen & Sons, Inc. v. City of Duluth, 225 Minn. 475, 481, 31 N.W.2d 270, 274 (1948)).

292. "It may be that the information Plaintiffs provided to Northwest was Plaintiffs' property. However, when that information was compiled and combined with other information to form a passenger name record (PNR), the PNR itself became Northwest's property." *Id.* at *4.

(5) Intrusion upon Seclusion Claim

Under Minnesota law, a plaintiff alleging intrusion upon seclusion must demonstrate that the defendant "intentionally intrude[d], physically or otherwise, upon the solitude or seclusion" of the plaintiff or his "private affairs or concerns" and that such intrusion "would be highly offensive to a reasonable person."[293] The court found that the plaintiffs voluntarily provided their personal information to Northwest and had a low expectation of privacy in that information.[294] Moreover, the court found that Northwest disclosed the information only to a government agency, as opposed to the public at large, with the intent of addressing security concerns following the 9/11 terrorist attacks.[295] Accordingly, the disclosure would not be highly offensive to a reasonable person and could not be the basis of a claim for intrusion upon seclusion.[296]

(6) Breach of Contract and Warranty Claims

Plaintiffs' breach of contract and warranty claims were based upon the privacy policy posted on Northwest's website, which indicated that when users of the website reserved or purchased travel services Northwest would "provide only the relevant information required by the car rental agency, hotel, or other involved third party to ensure successful fulfillment of your travel arrangements."[297] Though the plaintiffs did not allege that they actually read the privacy policy, they claimed to have "relied to their detriment" on the policy.[298]

The court held that Northwest's privacy policy was not a unilateral contract because it was not sufficiently definite and the plaintiffs did not allege that they had actually read the policy before providing their information to Northwest.[299] Instead, the court suggested that the privacy statement posted to Northwest's

293. *Id.* at *5 (citing Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 233 (Minn. 1998)).
294. *Id.* ("Plaintiffs [did] not contend that they actually read the privacy policy prior to providing Northwest with their personal information").
295. *Id.* ("Northwest's motives in disclosing the information cannot be questioned").
296. *Id.*
297. *Id.* at *5.
298. *Id.* at *6.
299. *Id.*

website was merely an unenforceable statement of policy.[300] Even if the policy statement was "sufficiently definite" and had been read by the plaintiffs before plaintiffs provided their information to Northwest, the court held that plaintiffs failed to allege any contract damages arising from the alleged breach.[301]

*b. North Dakota (*Dyer v. Northwest Airlines*)*

The North Dakota action was originally filed in state court, "alleg[ing] that Northwest's unauthorized disclosure of customers' personal information constituted a violation of the [ECPA], 18 U.S.C. §§ 2702(a)(1) and (a)(3), and a breach of contract."[302] Northwest removed the claims to federal court and filed a motion to transfer venue or to stay or dismiss the action, requesting "that the action be transferred to Minnesota," be stayed pending resolution of the Minnesota actions, or "dismissed for failure to state a claim upon which relief could be granted."[303]

The United States District Court for the District of North Dakota reviewed the plaintiff's claims under the standard for considering motions under Rule 12(b)(6) of the Federal Rules of Civil Procedure, accepting as true all of the factual allegations set forth in the complaint and construing the complaint in the light most favorable to the plaintiff.[304] In his response to Northwest's motion, the plaintiff conceded that, as a matter of law, no claim existed under 18 U.S.C. § 2702(a)(1) (which prohibits "a person or entity providing . . . an electronic communication service . . . to the public" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service").[305] Thus, the court was left to consider only the plaintiff's claims for violation of 18 U.S.C. § 2702(a)(3) (which prohibits a provider of "electronic communication service or remote computing service to the public" from "knowingly divulg[ing] a record or other information pertaining to a subscriber or customer of such service. . . to any governmental entity") and breach of

300. *Id.* The court noted that, under Minnesota law, "general statements of policy are not contractual." *Id.* (quoting Martens v. Minn. Mining & Mfg. Co., 616 N.W.2d 732, 741 (Minn. 2000)).
301. *Id.*
302. Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1197 (D.N.D. 2004).
303. *Id.*
304. *Id.* at 1198.
305. *Id.* (citation omitted).

contract.[306] These claims were dismissed.[307]

(1) ECPA Claim

Like the court in *Northwest*, the United States District Court for the District of North Dakota held that Northwest was not the provider of an "electronic communication service."[308] The court noted that "[i]n construing [the statutory definition of 'electronic communication service'], courts have distinguished those entities that sell access to the internet from those that sell goods or services on the internet" and that § 2702(a)(3) of the ECPA prescribed only the conduct of the former, an ISP or a "telecommunications compan[y] whose lines carry internet traffic."[309] Traditional online merchants and service providers are not providers of an "electronic communication service" under the ECPA.[310]

(2) Breach of Contract Claim

Like the plaintiffs in *Northwest*, the plaintiffs in *Dyer* contended that the privacy policy posted on the Northwest website constituted a contract which was breached when Northwest disclosed passenger information to NASA.[311] The breach of contract claim asserted in *Dyer* suffered the same fate as its predecessor: the court dismissed the claim on the grounds that the privacy policy was not a contract; the plaintiffs failed to allege that they accessed, read, understood, actually relied upon, or otherwise considered the privacy policy before providing their information to Northwest;[312] and the plaintiffs failed to allege actual damages arising from the alleged breach of contract.[313]

306. *Id.* at 1198–99 (citation omitted).
307. *Id.* at 1200.
308. *Id.* at 1199.
309. *Id.* at 1198–99.
310. *Id.* at 1199.
311. *See id.*
312. *See id.* at 1200. In this way, the complaint in *Dyer* was even more deficient than the complaint in *Northwest Airlines*, which at least alleged that the plaintiffs relied upon the privacy policy. *See* at *6 (D. Minn. June 6, 2004). *In re* Nw. Airlines Privacy Litig., No. Civ. 04-126(PAM/JSM), 2004 WL 1278459, at *6 (D. Minn. June 6, 2004).
313. *Dyer*, 334 F. Supp. 2d, at 1200.

2. American Airlines

American Airlines faced a nationwide class action lawsuit after authorizing the disclosure of passenger information to the Transportation Security Administration (TSA) without first obtaining the passengers' consent.[314] Plaintiffs filed suit against American, alleging that it had knowingly allowed unauthorized access to passengers' personal information and that its agent, Airline Automation, Inc. (AAI), had intentionally accessed and disclosed such information obtained from American's facility.[315] Specifically, plaintiffs alleged violations under the ECPA and state law claims for breach of contract, trespass to property, invasion of privacy, unjust enrichment, and deceptive trade practices.[316] In response, defendants filed a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), arguing that plaintiffs' complaint failed to state a claim for relief.[317] Finding that plaintiffs' claims were preempted by federal law or failed to state a claim, the court granted defendant's motion to dismiss all claims.[318]

a. ECPA Claim

Plaintiffs alleged that American's agent, AAI, violated § 2701 of the ECPA by accessing and disclosing plaintiffs' personal information from American's facility housing passengers' personal information.[319] Section 2701 prohibits "unauthorized access to a facility through which an electronic communication service is provided."[320] The court summarily dismissed the ECPA claim against AAI because American had authorized AAI to transfer the data, and therefore AAI's access was not unauthorized.[321] Similarly, the court rejected plaintiffs' argument that AAI violated § 2701 by exceeding its authorized access to American's facilities because the complaint relied only on the "theory of unauthorized *disclosure* of information, not of *access* that exceeded what was authorized."[322]

314. *See In re* Am. Airlines, Inc. Privacy Litig., 370 F. Supp. 2d 552, 554–55 (N.D. Tex. 2005).
315. *See id.* at 555.
316. *See id.* at 554, 562.
317. *See id.* at 554.
318. *Id.* at 554.
319. *See id.* at 558.
320. *Id.*
321. *See id.*
322. *See id.* at 559 ("Section 2701 does not proscribe unauthorized use or disclosure of information obtained from authorized access to a facility.").

Plaintiffs' claims against American for violation of § 2702 of the ECPA met a similar fate. American attempted to avoid liability under a statutory exception "which permits disclosure of electronic communications 'with the lawful consent of . . . an . . . intended recipient of such communication.'"[323] Plaintiffs argued that American's consent was unlawful because it violated American's privacy policy, which was part of the contract of carriage with passengers.[324] Noting that the ECPA § 2702 is "a criminal statute, and the mere breach of a contract normally is not 'unlawful' in a criminal sense,"[325] the court found that plaintiffs failed to state a claim against American under § 2702 of the ECPA.[326]

b. Breach of Contract Claim

Finding that plaintiffs' breach of contract was not expressly or impliedly preempted by the Airline Deregulation Act (ADA),[327] the court nevertheless found that plaintiffs' claim failed as a matter of law because plaintiffs alleged no damages as a result of the breach.[328] Although plaintiffs alleged "that they sustained injury as a result of defendants' deceptive practice and invasion of privacy," the court found that such damages failed to maintain a cause of action for breach of contract.[329]

c. State Law Claims

Under the ADA, state law "claims are preempted if they 'relate to' the prices, routes or services of an air carrier."[330] Plaintiffs asserted state laws claims for "trespass to property, invasion of privacy, deceptive trade practices, and unjust enrichment" in connection with American's disclosure of their personal information.[331] Finding that the personal information was obtained

323. *Id.* at 560 (citation omitted).
324. *See id.*
325. *Id.*
326. *Id.* at 561 ("Even if American was contractually bound by its privacy policy not to disclose passenger information and can be held liable for breach of contract, this obligation did not deprive it of the legal capacity under § 2702(b)(3) to consent to disclosure.").
327. *See id.* at 565–66.
328. *Id.* at 567.
329. *Id.*
330. *Id.* at 561–62 (internal quotation marks omitted) (quoting Lyn-Lea Travel Corp. v. Am. Airlines, Inc., 283 F.3d 282, 287 n.8 (5th Cir. 2002)).
331. *Id.* at 562.

in connection with American's "services," the court held that the ADA preempted plaintiffs' state law claims "because they have a connection at least with American's ticketing service, including the reservation component."[332]

3. JetBlue

JetBlue faced a similar class action brought by passengers whose personal information was transferred to a government contractor in connection with a Department of Defense (DOD) study regarding airline security in the wake of September 11, 2001.[333] Specifically, the DOD contractor, Torch Concepts, Inc. (Torch), sought JetBlue's "Passenger Name Records"[334] in order to create "a customer profiling scheme designed to identify high-risk passengers among those traveling on JetBlue."[335] After enlisting the help of the Department of Transportation and TSA, Torch successfully convinced JetBlue to hand over its passenger information, even though the transfer of such information violated the airline's own privacy policy.[336]

Plaintiffs, passengers whose personal information was disclosed to Torch, brought a class action against JetBlue, Torch, and others, alleging violations of the ECPA, New York General Business Law, breach of contract, trespass to property, and unjust enrichment.[337] Defendants subsequently filed a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) on the ground that plaintiffs had failed to state a claim for relief.[338] The United States District Court for the Eastern District of New York agreed,

332. *Id.* at 564 ("Congress surely intended to immunize airlines from a host of potentially-varying state laws and state-law causes of action that could effectively dictate how they manage personal information collected from customers to facilitate the ticketing and reservation functions that are integral to the operation of a commercial airline.").

333. *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

334. *Id.* at 304.

335. *Id.* at 305.

336. *Id.* at 305. The passenger information disclosed by JetBlue included "each passenger's name, address, gender, home ownership or rental status, economic status, social security number, occupation, and the number of adults and children in the passenger's family as well as the number of vehicles owned or leased." *Id.*

337. *Id.*

338. *Id.*

dismissing plaintiffs' claims.[339]

a. ECPA Claim

With respect to their ECPA claim, plaintiffs alleged that JetBlue's unauthorized disclosure of plaintiffs' personal information violated § 2702(a), prohibiting an electronic communication service from divulging the content of any communication maintained in electronic storage by that service.[340] Plaintiffs' claim hinged on whether JetBlue's Passenger Reservation Systems, the website maintained by JetBlue to facilitate passenger reservations, constituted an "electronic communication service" within the meaning of the ECPA.[341]

Similar to the Northwest cases, the court found that JetBlue did not provide an electronic communication service, and was "more appropriately characterized as a provider of air travel services and a consumer of electronic communication services."[342] In dismissing plaintiffs' ECPA claim, the court noted that the operation of its website did "not transform JetBlue into a provider of internet access, just as the use of a telephone to accept telephone reservations does not transform the company into a provider of telephone service."[343]

b. Violation of New York General Business Law

Plaintiffs' second argument was premised on the theory that by disclosing passenger information in direct violation of its own privacy policy, JetBlue engaged in an unfair or deceptive act in violation of New York General Business Law and other consumer protection statutes.[344] Defendants successfully argued that the

339. *Id.* at 330.

340. *Id.* at 306 (citing 18 U.S.C. § 2702(a) (1986)).

341. *Id.* at 306–07 (defining "electronic communication service" under the Electronic Communications Privacy Act (ECPA) as "any service which provides to users the ability to send or receive wire or electronic communications" (quoting 18 U.S.C. § 2510(15) (1986)).

342. *Id.* at 307–10. The court also found that JetBlue was not a "remote computing service" as defined under the ECPA and dismissed plaintiffs' claim under 18 U.S.C. § 2702(2) (1986). *Id.* at 310.

343. *Id.* at 307 ("Thus, a company such as JetBlue does not become an 'electronic communication service' provider simply because it maintains a website that allows for the transmission of electronic communications between itself and its customers.").

344. *Id.* at 315.

claim was preempted by federal law under the Airline Deregulation Act of 1978[345] because the adjudication of such a claim would directly impact the manner in which JetBlue communicated with its customers concerning reservations and ticket sales—conduct states are prohibited from engaging in under the ADA.[346]

c. Breach of Contract Claim

Plaintiffs based their breach of contract claim upon the theory that JetBlue's privacy policy formed a contract between the airline and its passengers not to disclose their personal information, and that by doing so, JetBlue breached that contract.[347] Although failing to persuade the court that the privacy policy was not a contract between the two parties but rather a "stand-alone privacy statement," JetBlue successfully dismissed the breach of contract claim on the ground that plaintiffs failed to allege damages resulting from the breach.[348] The court found that plaintiffs' only alleged damage, "loss of privacy," was not traditionally recognized in a breach of contract action.[349] Without demonstrating some economic loss as a result of the breach, plaintiffs' breach of contract claim was summarily dismissed.[350]

d. Trespass to Property

More accurately characterizing this claim as trespass to chattels, the court again was not persuaded by plaintiffs' argument that, by participating in the data transfer, defendants intentionally interfered with plaintiffs' personal property.[351] Critical to plaintiffs' claim was proving that the personal information transferred to Torch was in fact in the plaintiffs' possession.[352] Plaintiffs argued

345. 49 U.S.C. § 41713 (2006).

346. *JetBlue,* 379 F. Supp. 2d at 315–16 (applying the three-part *Rombom* test to determine preemption under the Airline Deregulation Act (ADA)).

347. *Id.* at 324–25.

348. *Id.* at 325–26.

349. *Id.* at 326.

350. *Id.* at 327 ("[Plaintiffs] had no reason to expect that they would be compensated for the 'value' of their personal information").

351. *Id.* ("To state a claim for trespass to chattels under New York law, plaintiffs must establish that defendants 'intentionally, and without justification or consent, physically interfered with the use and enjoyment of personal property in [plaintiffs'] possession,' and that plaintiffs were thereby harmed." (quoting Sch. of Visual Arts v. Kuprewicz, 771 N.Y.S.2d 804, 807 (2003))).

352. *Id.* at 327–29.

that JetBlue's privacy policy, limiting the airline's ability to transfer passenger information to third parties, granted them a possessory interest in the information because it could not be transferred without their consent.[353] While the court remained skeptical of plaintiffs' argument, it declined to decide the issue, instead dismissing the trespass claim because plaintiffs failed to establish actual injury as a result of the trespass.[354] Noting that the only injury alleged by plaintiffs was harm to their privacy interests, the court found that "such a harm [did] not amount to a diminishment of the quality or value of a materially valuable interest in their personal information."[355]

e. Unjust Enrichment

Similarly, the court found plaintiffs' unjust enrichment argument equally unconvincing. Alleging that JetBlue "received some form of remuneration from Torch or another party as a result of its disclosure of information," plaintiffs argued that the receipt of such compensation constituted unjust enrichment.[356] According to the airline, however, the only compensation it received as a result of the disclosure was "the potential for increased safety on its flights and the potential to prevent the use of commercial airlines as weapons that target military bases."[357] The court agreed with JetBlue, finding that the only benefit it received was indeed altruistic and dismissed plaintiffs' unjust enrichment claim as a result.[358]

V. NEW LEGISLATION SHOULD LEVERAGE PRIVATE ENFORCEMENT MECHANISMS

In an attempt to fill the void left by its failure to enact omnibus Internet privacy legislation, Congress delegated the responsibility for protecting our Internet privacy to the FTC.[359] Unfortunately, the FTC is unable to devote sufficient resources to fully address the

353. *Id.* at 327.
354. *Id.* at 328–29.
355. *Id.* at 329.
356. *Id.*
357. *Id.*
358. *Id.* at 330.
359. Children's Online Privacy Protection Act of 1998 § 1306, 15 U.S.C. § 6505 (2006); Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2006).

issue.[360] A few states have enacted statutes that may more effectively protect their citizens but the landscape formed by these enactments is uneven and replete with gaps, as the protections provided by each state (if they provide any protections at all) are different.[361]

Congress' enactment of omnibus Internet privacy legislation would provide a consistent standard for Internet privacy. To avoid over-burdening the FTC or any other governmental body, Congress should leave the enforcement of its new Internet privacy law to private citizens.

This concept is not new. Congress has long empowered private individuals to bring suit to "vindicate important public policy goals."[362] The idea behind this "private attorney general" concept is fairly simple, consisting "essentially of providing a cause of action for individuals who have been injured by the conduct Congress wishes to proscribe, usually with the additional incentive of attorney's fees for a prevailing plaintiff."[363] This concept has been used to address a variety of societal concerns, such as civil rights,[364] environmental protection,[365] securities fraud,[366] and the improper payment of Medicare funds.[367]

360. *See* Cody, *supra* note 198, at 1228.

361. *See supra* Part I.C.

362. Pamela S. Karlan, *Disarming the Private Attorney General*, 2003 U. ILL. L. REV. 183, 186 (2003) (discussing the concept of the "private attorney general").

363. *Id.*

364. Civil Rights Act of 1964 § 204, 42 U.S.C. § 2000a-3 (2006) (creating a private right of action to enforce public accommodation laws); Newman v. Piggie Park Enter., 390 U.S. 400, 401–02 (1968).

365. Federal Water Pollution Control Act § 505(a), 33 U.S.C. § 1365 (2006) (providing that "any citizen" may bring suit against any individual or company causing water pollution).

366. Securities Exchange Act of 1934 § 10(b), 15 U.S.C. § 78j (2006). The courts have found an implied private cause of action in this section. *See, e.g.*, Kardon v. Nat'l Gypsum Co., 69 F. Supp. 512, 513 (D.C. Pa. 1946) (using tort law principles to provide the basis for the plaintiff's cause of action); *see also* Sean G. Blackman, Note and Comment, *An Analysis of Aider and Abettor Liability Under Section 10(b) of the Securities Exchange Act of 1934:* Central Bank of Denver v. First Interstate Bank of Denver, 27 CONN. L. REV. 1323 (1995) (discussing the development of the private right of action under section 10(b)).

367. Social Security Act § 1862, 42 U.S.C. § 1395y(b)(3)(A) ("[Providing a private cause of action to recover damages] in the case of a primary plan which fails to provide primary payment (or appropriate reimbursement) in accordance with paragraphs (1) and (2)(A).").

In formulating a federal Internet privacy statute, Congress should be guided by the FTC's adoption of the core principles of fair information practices: Notice, Choice, Access, Security, and Enforcement.[368] Though these concepts are a reasonable starting place for our new statute, the first two are really the most important. In a free market economy, it seems that a website user who is fully and accurately *notified* of what personally identifying information a website collects, stores, and discloses; how, and for what purpose, such information is used; how such information is stored and protected; and to whom such information is going to be disclosed can make an educated *choice* about what, if any, information to reveal to the website. Like the statutes in California and Connecticut, our new federal Internet privacy law should require each[369] website operator to clearly and conspicuously display[370] a privacy policy that accurately notifies users of:

- what personally identifying information is collected, stored, or disclosed by the website;
- how, and for what purpose, such information is used by the website;
- how such information is stored and protected by the website; and
- to whom such information will or may be disclosed.

Each website should be required to handle personally identifying information only in accordance with its published privacy policy and should be prohibited from making false or misleading statements in such a policy.

Whenever the terms of a website's privacy policy materially change, each user of the site should be given the opportunity to "opt-out"[371] and require that the website handle his or her personally identifying information in accordance with the privacy

368. *Fair Information Practice Principles*, FED. TRADE COMM'N, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited June 30, 2011).

369. Requiring each website to display a privacy policy, as opposed to merely prohibiting sites from making false or misleading statements in such policies, will eliminate the disincentive for companies to adopt such policies posed by the laws in Nebraska and Pennsylvania. *See supra* Part II.C.

370. To ensure that users are given the opportunity to review the privacy policy, the law should require that a link to the policy be placed on the homepage of the website and each page which requests information from the user.

371. Our new federal statute would not require express "opt-in" consent to collect even sensitive information about an individual, thereby avoiding the concerns raised by industry groups about the draft Best Practices Act released by Representatives Boucher and Stearns. *See supra* Part II.B.3.

policy in effect at the time that the user revealed his or her information to the website. It seems only reasonable that the website operator who told his or her users that it would handle their information in a certain way before being given that information must not be permitted to enact an *ex post facto* policy change that may subject the users to risks they would not have voluntarily assumed.

Our new federal statute should proscribe minimum standards for a website's privacy practices and not preempt more protective state laws.[372] It must provide for a private cause of action for any person whose information has been handled by a website in a way that is materially inconsistent with the terms of that website's privacy policy or who has been harmed by relying upon a materially false or misleading statement set forth in such a policy.

Due to the difficulty in proving actual damages in Internet privacy cases, the new statute should provide for statutory damages, without proof of actual damages.[373] To encourage private citizens to bring suit to enforce their rights, and encourage competent attorneys to take on such suits, the new statute must require a court to award reasonable attorney's fees to a plaintiff who prevails in such an action.[374]

372. Thereby avoiding a primary objection, expressed by consumer groups, to the draft Best Practices Act released by Representatives Boucher and Stearns. *See supra* Part II.B.3.

373. Congress regularly provides for statutory damages where actual damages would be difficult to prove. *See, e.g.*, F.W. Woolworth Co. v. Contemporary Arts, Inc., 344 U.S. 228, 231 (1952) ("[Statutory damages are intended to allow] the owner of a copyright some recompense for injury done to him, in a case where the rules of law render difficult or impossible proof of damages or discovery of profits" (quoting Douglas v. Cunningham, 294 U.S. 207, 209 (1935))); Murray v. GMAC Mortg. Corp., 434 F.3d 948, 953 (7th Cir. 2006) (noting that statutory damages allow for the recovery of modest damages that are likely small and difficult to quantify, without proof of actual injury); Warner Bros., Inc. v. Dae Rim Trading, Inc., 877 F.2d 1120, 1126 (2d Cir. 1989) ("Statutory damages are awarded when no actual damages are proven or they are difficult to calculate.").

374. Karlan, *supra* note 362, at 205 ("Attorney's fees are the fuel that drives the private attorney general engine."). The underlying policy behind awarding attorney's fees is that it will encourage private individuals to bring the suit or encourage legal services organizations to bring such suits when the litigants themselves cannot afford to finance the litigation. *See id.* at 205–06; *see also* Brandenburger v. Thompson, 494 F.2d 885, 888 (9th Cir. 1974) (discussing attorney's fees in the context of the "private attorney general" doctrine).

VI. CONCLUSION

Our existing federal Internet privacy protections are insufficient. Congress has delegated the job of addressing our Internet privacy concerns to the FTC, and the FTC is unable to shoulder the entire burden. Only by spreading the burden amongst private citizens can the Internet privacy issue be fully addressed.

Congress should follow the lead of other nations in establishing an omnibus Internet privacy law that balances the needs of Internet users against those of the Internet businesses that drive the e-commerce economy. At a minimum, each website should be required to clearly and accurately inform its users of what personally identifying information it collects and how that information is used, stored, and disclosed. Armed with that knowledge, Internet users will be empowered to choose whether to reveal personally identifying information to websites that may disclose such information to third parties or use the information to generate revenue. By establishing appropriate minimum standards for Internet privacy, without diluting existing state law protections, and empowering individuals to enforce those standards by bringing suit, Congress will enhance our Internet privacy without placing an additional burden on the FTC or other government agencies.