PennState Dickinson Law

DICKINSON LAW REVIEW
PUBLISHED SINCE 1897

Volume 111
Issue 3 *Dickinson Law Review - Volume 111, 2006-2007*

1-1-2007

Online Privacy Policies: Contracting Away Control Over Personal Information?

Allyson W. Haynes

Follow this and additional works at: https://ideas.dickinsonlaw.psu.edu/dlra

Recommended Citation

Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 DICK. L. REV. 587 (2007).
Available at: https://ideas.dickinsonlaw.psu.edu/dlra/vol111/iss3/3

This Article is brought to you for free and open access by the Law Reviews at Dickinson Law IDEAS. It has been accepted for inclusion in Dickinson Law Review by an authorized editor of Dickinson Law IDEAS. For more information, please contact lja10@psu.edu.

Online Privacy Policies: Contracting Away Control Over Personal Information?

Allyson W. Haynes*

Table of Contents

I. Introduction

In the process of making an online purchase from "Webco," a website visitor named "Vi" discloses certain personal information, including her email address. Soon thereafter, Vi begins to receive numerous unsolicited emails from various advertisers seeking her business. Has Webco violated the law by sharing or even selling Vi's

* Assistant Professor of Law, Charleston School of Law. J.D., *magna cum laude*, University of South Carolina School of Law; B.A., Duke University.

email address? The answer may lie not in state or even federal legislation, but in a contract that Vi unwittingly entered into when she made the online purchase. In addition, Vi may have agreed that if any dispute arises concerning the use of her personal information, she must arbitrate that claim—again based on an agreement of which she was unaware. Online privacy policies increasingly purport to govern what can be done with website visitors' personal information.[1] Are they in fact binding contracts?

Whether an online visitor discloses personal information in the course of a purchase or simply because the visitor wishes to receive information in the future, that disclosure is likely the subject of an online privacy policy. Increasingly, privacy policies have become the place where website operators can limit their liability for certain treatment of personal information by disclosing that they might in fact do exactly that.[2] The current legal framework governing privacy policies gives great importance to the concepts of notice and truthful disclosure[3]—i.e., is the website treating a consumer's personal information the way the site promised it would when the consumer provided its personal information to the site? In fact, if the website complies with its own promises, there is little else to prevent the site from doing with the information whatever it wants—sharing, selling or otherwise making use of the information—besides the website company's own interest in attracting and maintaining customers.[4]

The risk to the website, of course, is that a potential customer will choose not to do business with a particular website that fails to treat his or her personal information in a particular manner.[5] However, most studies show that, while consumers are increasingly concerned about the privacy of their personal information, they are still not likely to read—much less understand—online privacy policies.[6] This increases the

1. *See infra* Part II.B.1.

2. *See infra* Part IV; Anthony D. Miyazaki & Ana Fernandez, *Internet Privacy and Security: An Examination of Online Retailer Disclosures*, 19 J. PUB. POL'Y & MARKETING 54, 58 (2000) (finding only 17% of commercial websites surveyed disclosed that they would *not* share personal information with third parties).

3. *See infra* note 86 and accompanying text.

4. *See infra* Part III; *but see infra* Part IV (most consumers do not read privacy policies).

5. Customers are finding out about these breaches more often now that legislation requires notification. *See infra* note 86. As a result, consumers may boycott websites that disclose personal information. Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1286 (2005).

6. "In a study of adult Internet users who were asked to evaluate the credibility of Web sites, less than one percent of respondents even noticed privacy policies." James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 11 (2005)

incentive of a website operator to disclose the potential for broad use of personal information, even if such use is not currently contemplated.[7]

This article discusses such privacy policies from a contract perspective: do they create a binding contractual relationship with the consumer? What are their terms? Do they actually increase a consumer's online privacy? If not, can consumers challenge the enforceability of those policies?

Part II discusses how privacy policies have evolved in light of the increase in websites' use of them and the growing attention to the issue of online privacy in general. Part III discusses the legal framework that governs the posting of privacy policies—both procedural requirements for the posting of privacy policies and more substantive controls over the use of personal information disclosed by online customers—which results in the law being notice-based rather than focused on the substantive use of personal information. Part IV discusses the disconnect between the growing attention to online treatment of personal information, and actual consumer awareness of how websites treat their personal information. The potential for a website to lose customers based on provisions in their privacy policies is low,[8] and privacy policies are likely to provide less, rather than more, privacy protection as website operators give themselves the option of sharing or selling customer information. In addition, privacy policies are likely to include other terms that are unfavorable to consumers, including arbitration and forum selection clauses.

(citing B.J. FOGG, ET AL., HOW DO PEOPLE EVALUATE A WEB SITE'S CREDIBILITY?: RESULTS FROM A LARGE STUDY 1, 86 (2002), http://www.consumerwebwatch.org/pdfs/stanfordPTL.pdf). Researchers have found that "online information privacy is important to consumers and that consumers desire more control over access to their personal information and subsequent use of the information after it is obtained," Nehf at 5, which would suggest that consumers would take steps to protect their privacy by frequenting websites that have favorable policies and avoiding those that do not. However, "research on bounded rationality and consumer decision making suggests that in most circumstances consumers, acting rationally, do not factor privacy policies into their decision processes, even when they consider privacy important, because privacy concerns are seldom salient." *Id. See also* M.J. Culnan & G.R. Milne, *The Culnan-Milne Survey of Consumers and Online Privacy Notices: Summary of Responses* 1, 2 (2001), http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf (consumers still do not seem to read online privacy policies); Humphrey Taylor, *Most People Are "Privacy Pragmatists" Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits*, THE HARRIS POLL No. 17, March 19, 2003, http://www.harrisinteractive.com/harris_poll/index.asp?PID=365.

7. *See* Mary J. Hildebrand & Jacqueline Klosek, *Recent Security Breaches Highlight the Important Role of Data Security in Privacy Compliance Programs*, 17 INTELL. PROP. & TECH. L.J., May 2005, at 20, 20-21 (recommending that companies allow themselves the leeway in their privacy policies to share information in ways they may not anticipate).

8. Nehf, *supra* note 6, at 5.

In light of the possibility that consumers will wish to avoid being bound by such a policy if a dispute does arise, Part V looks at their enforceability. Like other online agreements, privacy policies are more likely to bind consumers if they are entered into via "clickwrap" and their terms are not otherwise unconscionable. Because privacy policies are often presented via "browsewrap,"[9] consumers have a strong argument for challenging their enforceability. In addition, specific terms of privacy policies—such as arbitration and forum selection clauses—are open to claims of unconscionability.

II. Privacy Policies and the Online Trade in Personal Information

A. Online Provision of Personal Information

Personal information[10] is provided by website visitors[11] in numerous ways. From the simple act of providing an email address for the purpose of receiving an email newsletter,[12] to the provision of a credit card number and mailing address to facilitate a purchase,[13] to the most risky

---

9. *See* Robert A. Hillman & Jeffrey J. Rachlinski, *Standard Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 431 (2002) (describing increasing occurrence of "clickwrap" contracts and attempts by businesses to create "browsewrap" contracts).

10. The term "personal information" is used here as it is defined under federal law:

> [I]ndividually 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.

Children's Online Privacy Protection Act of 1998, 15 U.S.C.A. § 6501(8) (West Supp. 2006).

In the financial realm, federal law defines nonpublic personal information as "personally identifiable financial information—(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." Gramm-Leach-Bliley Act of 1999, 15 U.S.C.A. § 6809(4) (West Supp. 2006); *see also* 18 U.S.C.A. § 2725(3) (West 2000) ("'[P]ersonal information' means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.").

11. The website visitor who provides his or her personal information to a website is variously referred to in this article as a "visitor," "user," or "consumer."

12. For example, L.L.Bean's website invites visitors to "Sign up for our Email Newsletter and learn about our latest products and sale events. It's easy to subscribe—just enter your email address below." L.L.Bean: Email Newsletter, http://www.llbean.com (follow "Email Newsletter" hyperlink) (last visited Jan. 31, 2007).

13. Like many retail sites, Target.com allows a user to create an account including

provision of social security numbers and other financial information to a bank in order to apply for a loan,[14] personal information is given freely and often in the ever-growing online American market.[15]

There is growing attention to the security that websites afford such personal information[16] in the wake of recent high-profile personal information disasters, such as the theft of personal information from a Veterans Administration employee, putting at risk the identities of over two million active-duty military personnel;[17] AOL's recent disclosure of search data entered by more than 650,000 subscribers;[18] and the security breach at LexisNexis resulting in improper access to personal information belonging to about 310,000 people.[19] These events have attuned the public to the importance of the security with which personal information is stored, and the resulting risk of identity theft if such information is lost or stolen.[20]

---

the user's mailing address and credit card number so that the user can conveniently make a purchase with only one click of her mouse. *See* Target.com: My Account, http://www.target.com (follow "my account" hyperlink) (last visited Jan. 31, 2007).

14. *See* CitiFinancial: What You Can Expect, https://secure.citifinancial.com/common/whatyoucanexpect.php (last visited Jan. 31, 2007).

15. In 2005, total e-commerce sales in the United States were estimated at $86.3 billion, an increase of 24.6% from 2004. These online sales accounted for 2.3% of total sales in the country, up from 2.0% of total sales in 2004. U.S. Census Bureau News, Quarterly Retail E-commerce Sales, 4th Quarter 2005 (Feb. 17, 2006), http://www.census.gov/mrts/www/data/html/05Q4.html.

16. There has also been increased attention to the threat of online sexual predators, particularly those who target children. *See* Chelsea Kellner, *Web Site Builds Web of Friends*, PITTSBURGH TRIBUNE-REVIEW, Feb. 7, 2006, at E4 (discussing how websites like Myspace.com and Facebook.com pose challenges to law enforcement because they allow predators to identify young people by the personal information they provide); *SAFE ONLINE: History of Local Stories*, EYEWITNESS NEWS, http://www.eyewitnessnewstv.com (hover over "Special Reports" hyperlink; then hover over "Know More Links" hyperlink; then follow "Archived Story Links" hyperlink; then follow "SAFE ONLINE: History of Local Stories" hyperlink) (last visited Jan. 31, 2006) (discussing recent stories about friend-networking websites like Myspace, and adults pursuing children online).

17. *See* Hope Yen, *Data on 2.2M Active Troops Stolen from VA*, ABC NEWS, June 6, 2006, http://www.abcnews.go.com (search for "Data on 2.2M Active Troops Stolen from VA") (noting that records on file for almost all active-duty personnel—including as many as 1.1 million active-duty personnel from all the armed forces, along with 430,000 members of the National Guard, and 645,000 members of the Reserves—had been stolen in what has become "one of the nation's largest security breaches").

18. *See* Saul Hansell, *AOL Removes Search Data on Vast Group of Web Users*, N.Y. TIMES, Aug. 8, 2006, at C4 (describing AOL's release of Internet search terms from more than 650,000 subscribers over a three-month period and its acknowledgement that the search queries themselves may contain personally identifiable information).

19. *See* David Colker, *LexisNexis Breach Is Larger: The Company Reveals that Personal Data Files on as Many as 310,000 People Were Accessed*, L.A. TIMES, Apr. 13, 2005, at C1.

20. *See generally* Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Jan. 31, 2007)

This article focuses on a different kind of risk—the risk that a visitor will unwittingly agree to allow a company to share or sell her personal information to third parties. Such disclosure can also result in identity theft,[21] as well as contribute to the less pernicious, but thoroughly irritating and often expensive, increase in spam.[22]

Concern over online personal privacy has grown from 43% of respondents being "very concerned" and 35% being "somewhat concerned" about threats to their personal privacy in 1990,[23] to an overwhelming 88% of 1,500 Internet users being very or somewhat concerned about websites' collection of personal information in 2003.[24] The issue of personal information privacy even promises to be a factor in

---

(maintaining a running total of records compromised by security breaches). To date, over 100 million records have been put at risk as a result of security breaches at companies holding sensitive consumer information. *Id.*; *see also Data Theft Due to Criminal Intent is a Reality Now*, FIN. EXPRESS, July 25, 2005, *available at* 2005 WLNR 11611049 (discussing security breach of cardholder information held by Cardsystems); *Another Week, Another Identity Theft Scandal: Recent Data Security Breaches Underscore Need for Stronger Identity Theft Protections*, http://www.consumersunion.org/creditmatters/creditmattersupdates/002244.html (describing recent security breaches of information owned by LexisNexis, ChoicePoint, Bank of America, and Ameritrade among others and detailing protection laws that Consumer Union is attempting to enact) (last visited Jan. 31, 2007).

21. An example is the sale by ChoicePoint, one of the country's largest data brokers, of personal data of approximately 162,000 individuals to identity thieves. *See* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 (2006) (describing the ChoicePoint debacle); Michael Hiltzik, *Big Data Broker Eyes DMV Records*, L.A. TIMES, Dec. 1, 2005, at C1 (noting that ChoicePoint not only sold personal information of 162,000 people to L.A. identity thieves but also has been accused of such unauthorized sales before); Joseph Menn, *Did the ChoicePoint End Run Backfire?*, L.A. TIMES, Mar. 13, 2005, at C1 (describing the ChoicePoint incident and predicting tighter regulation on collection of personal data); Bob Sullivan, *Database Giant Gives Access to Fake Firms: ChoicePoint Warns More than 30,000 They May be at Risk*, MSNBC, Feb. 14, 2005, http://www.msnbc.msn.com/id/6969799 (detailing ChoicePoint incident and the risks consumers face as a result of security breach).

22. According to Jupiter Research, "American consumers will receive an estimated 645 billion commercial email messages in the year 2007." Linda A. Goldstein, *Online Advertising: Rules of the Net*, 822 PLI/PAT 291, 325 (2005). Congress has recognized that "[t]he convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail," and that such mail "may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail" as well as impose "significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and receive such mail." Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 2(a), 117 Stat. 2699, 2699 (2003).

23. *Public Opinion on Privacy*, ELEC. PRIVACY INFO. CTR., http://www.epic.org/privacy/survey/ (last visited Jan. 31, 2007) (citing *Privacy in America and Consumers in the Information Age*, THE HARRIS POLL, January 1990 (study number 892049)).

24. Anne Kandra & Andrew Brandt, *The Great American Privacy Makeover*, 21 PC WORLD, Oct. 8, 2003, at 145-146, *available at* http://www.pcworld.com/article/id,112468-page,1-c,privacy/article.html.

the 2008 presidential election.[25] However, the legislative solution—online privacy policies—may actually decrease protection of consumer information by encouraging websites to protect themselves instead.

B. Privacy Policy Terms

Online privacy policies have appeared all over the Internet both in response to increases in legislation requiring such disclosure,[26] and as a voluntary measure[27] by websites to appeal to consumers by emphasizing the care with which they treat consumer information.[28] In 1998, only 2% of all websites had some form of privacy notices,[29] and in 1999, eighteen of the top 100 shopping sites did not display a privacy policy.[30] By 2001, virtually all of the most popular commercial websites had privacy notices,[31] with the number continuing to increase through 2005.[32] Today

25. *Cf. Clinton Touts Privacy Bill of Rights*, NEWSDAY, June 17, 2006, at A16 ("[Senator] Clinton wants a 'privacy czar' within the White House to guard against recent problems like the recent theft of personal data from Department of Veterans Affairs. She also wants legislation to let consumers know what information companies are keeping about them and how it is used, and . . . with penalties for companies who are not careful with personal data.").

26. *See infra* Part III.B.

27. *See Information Privacy: The Current Legal Regime*, The Business Roundtable, 1, 4 (2001) [hereinafter "Business Roundtable Report"], *available at* http://64.203.97.43/pdf/617.pdf (noting that businesses may provide privacy policies "as a voluntary measure to protect consumer privacy"); *see also* Hildebrand & Klosek, *supra* note 7, at 20 ("Companies that collect, use, and/or process Personal Data are also under increasing pressure from consumers to provide clear and complete information regarding their policies and practices relative to the collection, use, and disclosure of Personal Data. As a result, many entities, even those that are not under any legal obligation to do so, have been developing and posting Web site privacy policies.").

28. *See* Nehf, *supra* note 6, at 1-2 ("Market pressures encourage many businesses to at least appear sensitive to customers' privacy concerns. Most businesses would like to avoid the perception or implication that they harvest and sell the personal data they obtain either openly or surreptitiously from their customers. Indeed, business consulting firms now routinely encourage the adoption and promotion of privacy policies as a way to present a positive client image. Appearing concerned about customer privacy has become a standard marketing strategy.").

29. *See* Timothy J. Muris, Chairman, Fed. Trade Comm'n, Protecting Consumers' Privacy: 2002 and Beyond, Remarks at the Privacy 2001 Conference (Oct. 4, 2001), *available at* http://www.ftc.gov/speeches/muris/privisp1002.htm.

30. *Surfer Beware III: Privacy Policies without Privacy Protection*, ELEC. PRIVACY INFO. CTR. (1999), http://www.epic.org/reports/surfer-beware3.html.

31. *See Challenges Facing the Federal Trade Commission: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 107th Cong. 22 (2001) (statement of Timothy J. Muris, Chairman, Fed. Trade Comm'n). "One of the things that is under-appreciated by some is the extent to which there has been considerable progress in posting privacy policies. All of the top web sites have such policies." *Id.*

32. More companies had online privacy policies and secure online forms in 2005 than in 2004. Alorie Gilbert, *Companies Dinged on Web Privacy*, CNET NEWS.COM, August 23, 2005, http://news.com.com/2100-1029_3-5842176.html (discussing the

it is rare to visit a website that does not have a privacy policy, although there are certain industries—like higher education—that lag behind in posting such policies.[33]

Typical privacy policies are accessed via hyperlinks at the bottom of the screen on a website's home page.[34] They notify users about the type of personal information they collect, the purposes for that collection, how that information is used, and the security with which that information will be handled.[35] For example, America Online's AOL Network Privacy Policy tells its registered users that the information gathered about them may include "registration-related information (such as name, home or work addresses, e-mail addresses, telephone and fax numbers, birth date or gender)," information about users' visits to AOL websites, users' responses to offerings and advertisements, users' searches and how those searches are used, "transaction-related information" including credit card and other billing information and purchase history, and customer service information.[36]

1. Use of Personal Information

Importantly, privacy policies describe the ways in which the website will use the visitor's personal information.[37] In a typical provision, AOL users are told that the personal information collected by AOL may be shared with its "affiliated providers,"[38] and with third parties if it is

---

Customer Respect Group 2005 Privacy Report).

33. *Bentley College-Watchfire Survey of Online Privacy Practices in Higher Education Reveals Risk Management Issues for U.S. Colleges and Universities*, April 24, 2006, http://www.watchfire.com/news/releases/04-24-06.aspx ("[W]hile most schools engage in e-commerce, only 65 of 236 schools surveyed have privacy notices linked from their home page while nearly all schools surveyed engage in practices that potentially pose a privacy risk."). In addition, it is estimated that while many churches post a great deal of personal information online, less than 3% of church websites post a privacy policy. Mariea Grubbs Hoy & Joseph Phelps, *Consumer Privacy and Security Protection on Church Web Sites: Reasons for Concern*, 22 J. PUB. POL'Y & MARKETING 58, 67 (2003).

34. *See, e.g.*, Semtech.com, *infra* note 42 and accompanying text.

35. *See infra* Part II.B.1.

36. AOL Network Privacy Policy, http://about.aol.com/aolnetwork/aol_pp (last visited Jan. 31, 2007). AOL further describes to users its "Commitment to Security," having "established safeguards to help prevent unauthorized access to or misuse of your AOL Network information," and using passwords to verify user identity. *Id.* However, AOL notes that it "cannot guarantee that your personally identifiable information will never be disclosed in a manner inconsistent with this Privacy Policy." *Id.*

37. The greater the amount of sharing and/or selling of such information to third parties, the greater the risk to that information's security and the greater the likelihood that the website visitor will receive unsolicited email. *See generally Spam: Unsolicited Commercial E-mail*, ELEC. PRIVACY INFO. CTR., http://www.epic.org/privacy/junk_mail/spam/ (last visited Jan. 31, 2007); *Surfer Beware, supra* note 30.

38. Via hyperlink, users are told "[t]he AOL Network's affiliated providers include,

"necessary to fulfill a transaction," based on the user's consent, or "except as described in this Privacy Policy."[39]

Similarly, Amazon.com tells its users that it is not "in the business of" selling personal information, but that it may share personal information with third parties in relation to transactions with those parties, with third-party service providers, with other businesses pursuant to promotional offers, or in the process of buying or selling stores or other business units.[40] USATODAY.com tells its visitors that it "reserve[s] the right to use and to disclose to third parties all of the information that we collect online about you and other visitors in any way and for any purpose," except that it will not email promotional offers "directly" to the user unless that user has specifically agreed to receive such promotional materials.[41] Other companies reserve the right to provide users' personal information to third parties for various purposes,[42] to send email marketing to their users, [43] and even to sell users' personal information.[44]

2. Dispute Resolution and Other Terms

Online privacy policies include more than just "privacy" terms.

---

or will soon include: AOL Internet Phone Service (AOL Enhanced Services L.L.C.)[.] The AOL Network may in the future designate other affiliated providers." AOL Network, Affiliated Providers, http://about.aol.com/aolnetwork/affiliates.html (last visited Jan. 31, 2007).

39. AOL Network Privacy Policy, *supra* note 36.

40. Amazon.com Privacy Notice, http://www.amazon.com (follow "Privacy Notice" hyperlink) (last visited Jan. 31, 2007).

41. USATODAY.com Privacy Policy, http://www.usatoday.com/marketing/privacy-policy.htm (last visited Jan. 31, 2007). For a discussion of the extent to which such "opt-out" clauses actually increase consumer choice, *see* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

42. *See* 11Alive.com Privacy Policy, http://www.11alive.com/company/about_us/legal/privacy.aspx (last visited Jan. 31, 2007) ("Unless you inform us in accordance with the process described below, we reserve the right to use, and to disclose to third parties, all of the information collected from and about you while you are using the Site in any way and for any purpose, such as to enable us or a third party to provide you with information about products and services."); Semtech.com Website Privacy Policy, http://www.semtech.com (follow "Privacy Policy" hyperlink) (last visited Jan. 31, 2007) ("Under certain circumstances, we may provide your personal information to third parties for the purpose of delivering our goods or services to you and for other purposes related to your use of our products or your interest in securing employment with Semtech.").

43. *See* AzoogleAds Privacy Policy, http://offers.blinko.com/privacy.htm (last visited Jan. 31, 2007) ("By submitting your e-mail address at the Website you agree to receive e-mail marketing from Blinko and our third-party advertisers.").

44. *Id.* "We may sell our user information and/or join together with other businesses to bring selected opportunities to our users. We are able to offer third party services to you, in part, based on your willingness to be reached by our third-party advertisers." *Id.*

AOL's privacy policy is typical in that it is incorporated by reference in the Aol.com Terms of Use.[45] Those Terms of Use include a disclaimer of warranties,[46] limitation of liability,[47] and a designation of the Commonwealth of Virginia as governing the law and location for resolving any claim or dispute the user may have against AOL.[48] Amazon.com's Privacy Notice states: "If you choose to visit Amazon.com, your visit and any dispute over privacy is subject to this Notice and our Conditions of Use, including limitations on damages, arbitration of disputes, and application of the law of the state of Washington."[49]

3. Binding Nature of the Policy and Amendments Thereto

While the legislation that requires privacy policies focuses on disclosure of website practices in order to increase consumer awareness, most websites in fact present these policies and amendments thereto as binding upon visitors, using the language of contract and assent. AOL's Terms of Use state: "Your ongoing use of AOL.COM signifies your consent to the information practices disclosed in our Privacy Policy."[50] AOL reserves the right to change the Terms of Use at any time, and advises the user that he is "responsible for checking these terms periodically for changes."[51] Users are deemed to have accepted the new terms by continuing to use AOL.COM after changes are posted to the Terms of Use.[52] Similarly, Amazon.com's privacy policy tells its users that "[b]y visiting Amazon.com, you are accepting the practices

45. AOL.com's Terms of Use state: "YOUR AFFIRMATIVE ACT OF USING AOL.COM SIGNIFIES THAT YOU AGREE TO THE FOLLOWING TERMS OF USE, YOU CONSENT TO THE INFORMATION PRACTICES DISCLOSED IN THE AOL NETWORK PRIVACY POLICY, AND YOU CONSENT TO RECEIVE REQUIRED NOTICES AND TO TRANSACT WITH US ELECTRONICALLY. IF YOU DO NOT AGREE, DO NOT USE AOL.COM." AOL.com Terms of Use, http://about.aol.com/aolnetwork/aolcom_terms (last visited Jan. 31, 2007).

46. *Id.*

47. *Id.*

48. *Id.*

49. Amazon.com Privacy Notice, *supra* note 40.

50. AOL.com Terms of Use, *supra* note 45.

51. *Id.*

52. *Id.* Interestingly, in France, where the European Union Unfair Terms Directive has been implemented, a court found that thirty-one clauses in AOL's Internet service agreement were unfair or illegal, including those that allowed AOL to transmit the subscriber's personal information to third parties without the subscriber's prior consent. *See* Juliet M. Moringiello & William L. Reynolds, *Survey of the Law of Cyberspace: Internet Contracting Cases* 2004-2005, 61 BUS. LAW. 433, 444 (2005) (discussing Union Fédérale des Consommateurs Que Choisir v. AOL, T.G.I. Nanterre, J.C.P. 2004 II, 10022, note Fages).

described in this Privacy Notice."[53]

USA Today tells its online readers, "By visiting and using the Site, you agree that your use of our Site, and any dispute over privacy, is governed by this Privacy Policy and our Terms of Service."[54] USA Today also reserves the right to change the policy at any time, without notice:

> Because the Web is an evolving medium, we may need to change our Privacy Policy at some point in the future, in which case we'll post the changes to this Privacy Policy on this website and update the Effective Date of the policy to reflect the date of the changes. By continuing to use the Site after we post any such changes, you accept the Privacy Policy as modified.[55]

Thus, the typical privacy policy purports to bind the consumer, finding consumer consent by the consumer's use of the website or provision of information. And the typical privacy policy includes, or incorporates by reference, a slew of terms both relating to privacy (and often allowing sharing and multiple uses of personal information) and relating to other rights of the consumer—notably, the right to bring suit in the consumer's forum of choice.

III. Privacy Policies and the Law

As applied to most commercial websites, the existing legislation requires that a privacy policy be posted, and that the entity abide by that policy, but does not regulate the substance of that policy.[56] No law prevents a website operator from sharing or selling personal information it has lawfully been given, although a website can be held liable for failing to notify its customers of its practice of selling or sharing such information.[57] As long as they comply with the disclosure requirement,

---

53. Amazon.com Privacy Notice, *supra* note 40; *see also* Bankrate.com Privacy Policy, http://www.bankrate.com/coinfo/privacy.asp (last visited Jan. 31, 2007) ("By visiting, using and/or submitting information to www.bankrate.com, you are accepting the practices described in this Privacy Policy and the terms and conditions of Bankrate's Agreement of Terms of Use located at the URL www.bankrate.com/brm/about/disclaimer.asp (the "Terms of Use").").

54. USATODAY.com Privacy Policy, *supra* note 41.

55. *Id.*

56. *See* Nehf, *supra* note 6, at 3-4 ("Policies might disclose how data is collected and how it will be transferred, sold, or traded, but often the message is that information will be collected in whatever way the Web site can obtain it, and the site reserves the right to share or sell it with impunity.").

57. This is consistent with an apparent trend in online contracting case law where courts focus on procedure rather than substance. Moringiello & Reynolds, *supra* note 52, at 434 (noting that in cases during 2004 and 2005, courts discussed "whether the buyer had reasonable notice of the on-line terms restricting her rights," but not "whether those terms, assuming reasonable communication, were substantively fair").

websites are free to state in their privacy policies that they will treat a visitor's personal information virtually any way they wish, arguably immunizing themselves from liability for such treatment.[58]

A. Federal Law

Existing federal legislation governs the treatment of personal information by regulating specific types of entities and specific types of information. For example, federal law regulates the collection, maintenance and dissemination of personal information by "consumer reporting agencies,"[59] protects "customer proprietary network information" from disclosure by telecommunications carriers,[60] regulates how federal governmental agencies gather and handle personal data,[61] and requires financial services companies to implement measures to protect the security and confidentiality of their customers' personal information.[62] In addition, legislation restricts the use and disclosure of certain specific types of personal information, including individually identifiable health information,[63] education records,[64] and consumer reports.[65]

Federal legislation also specifically aims at dissemination of information held in an electronic format. The "CAN-SPAM Act" regulates the treatment of personal information in the form of email addresses by prohibiting the sending of "unsolicited" email and of misleading header information.[66]

---

58. *See supra* Part III.A. (discussing legislative exceptions). Commentators have decried the "absence of U.S. laws to control much of the extraction, manipulation, and sharing of data about people and what they do online." JOSEPH TUROW, AMERICANS & ONLINE PRIVACY: THE SYSTEM IS BROKEN, A REPORT FROM THE ANNENBERG PUBLIC POLICY CENTER OF THE UNIVERSITY OF PENNSYLVANIA 5 (2003) ("[With limited exceptions,] online companies have virtually free reign to use individuals' data in the U.S. for business purpose without their knowledge or consent. They can take, utilize and share personally identifiable information—that is, information that they link to individuals' names and addresses. They can also create, package and sell detailed profiles of people whose names they do not know but whose interests and lifestyles they feel they can infer from their web-surfing activities.").

59. Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681-1681x (West 1998 & Supp. 2006).

60. 47 U.S.C.A. § 222 (West 2001 & Supp. 2006).

61. Privacy Act of 1974, 5 U.S.C.A. § 552a (West 1996 & Supp. 2006).

62. Gramm-Leach-Bliley Act, 15 U.S.C.A. §§ 6801-6809 (West Supp. 2006).

63. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C.A. § 1320d-2 (West 2003).

64. Family Education Rights and Privacy Act, 20 U.S.C.A. § 1232g (West 2000 & Supp. 2006).

65. Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681-1681x (West 1998 & Supp. 2006).

66. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C.A. §§ 7701-7713 (West Supp. 2006). Of course, if

The Computer Fraud and Abuse Act is aimed at computer hackers and prohibits unauthorized access to a "protected" computer (one that is used by a financial institution or in interstate commerce).[67] Title I of the Electronic Communications Privacy Act ("ECPA") is aimed at protecting the privacy of communications by prohibiting the interception of electronic communications.[68] Importantly, there is a statutory exception to the Act "where one of the parties to the communication has given prior consent to such interception."[69] Such "prior consent" could come from the website's privacy policy.

Title II of the ECPA (also known as the "Stored Communications Act") prevents improper access to "stored" electronic communications,[70] but does not speak to use of that information.[71] Again, there is a statutory exception for communications divulged "with the lawful consent of the originator or an addressee or intended recipient of such communication."[72]

In addition, the Federal Trade Commission ("FTC") interprets Section 5 of the FTC Act[73]—which prohibits unfair or deceptive acts or practices—as applying to a company's misrepresentations or failure to abide by its own privacy policy statements.[74] The Act does not require a privacy policy, but provides a means of enforcement of a policy's terms if the company does have one. The FTC has also applied Section 5 to websites' misuse of personal information in the absence of a posted privacy policy pursuant to the "unfair" rather than "deceptive" prong of

---

a website company's privacy policy provides that a visitor agrees to receive email communications, the company does not violate the Act by sending email.

67. 18 U.S.C.A. § 1030(a)(2)(C) (West 2000 & Supp. 2006).

68. *Id.* §§ 2710-2712. *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003). The legislation provides a private right of action against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C.A. § 2511(1)(a) (West 2006). To "intercept" a communication, a party must acquire the contents of such a communication "through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). Such "contents" have been found to include personally identifiable information. *Pharmatrak*, 329 F.3d at 18 (citing Gelbard v. United States, 408 U.S. 41, 51 n.10 (1972)).

69. 18 U.S.C.A. § 2511(2)(d) (West 2006).

70. *Id.* §§ 2701-2712. The statute provides that a person or entity providing either an electronic communication service or a remote computing service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service. *Id.* § 2702.

71. Specifically excluded from the statute is "conduct authorized . . . by the person or entity providing a wire or electronic communications service" or "by a user of that service with respect to a communication of or intended for that user. . . ." *Id.* § 2701(c).

72. *Id.* § 2702(b)(3).

73. 15 U.S.C.A. § 45(a)(1)-(2) (West 1997).

74. *See infra* Part IV.C. and cases discussed therein.

the statute.[75]

In the past, there has been a push by the federal government to regulate the substance of websites' treatment of personal information in addition to requiring that certain entities disclose that treatment.[76] But the proposed legislation was not adopted, and the FTC determined instead to follow the existing self-regulation model, it being "the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology."[77] The remains of that proposed substantive legislation are now in the form of "best practices guidelines" or "fair information practices" that encourage disclosure and recommend other privacy practices like security measures and consumer options.[78]

Other aspects of the so-called self-governance model of U.S. privacy policy include privacy seals of approval,[79] voluntary pledges by

---

75. *See In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465, 2005 FTC LEXIS 134 (2005).

76. The FTC issued a report to Congress examining the issue of online privacy in 2000, which stated that "ongoing consumer concerns regarding privacy online and limited success of self regulatory efforts to date make it time for government to act to protect consumers' privacy on the Internet." *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 28-29 (2000), *available at* http://www.ftc.gov/reports/ privacy2000/privacy2000.pdf. The FTC voted three to two to recommend that Congress enact legislation to ensure adequate protection of consumer privacy by requiring all consumer-oriented websites that collect personal identifying information to establish privacy policies in accordance with the four "Fair Information Practice Principles" ("FIPP"). *Id.*

77. Self-Regulation & Privacy Online: Statement Before the House Commerce Subcomm. on Telecomm., Trade, and Consumer Prot. of the H. Comm. on Commerce, 106th Cong. (1999), available at http://www.ftc.gov/os/1999/07/pt071399.htm (statement of the Federal Trade Commission). By 2001, FTC Chairman Timothy J. Muris noted that a majority of the Commission was not in favor of online privacy legislation at that time. Challenges Facing the Fed. Trade Comm'n: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce, 107th Cong. (2001) (statement of Timothy J. Muris, Chairman, Federal Trade Commission), 2001 WL 1383075; *see also* Nehf, *supra* note 6, at 3 (describing how self-regulation resulted from the FTC's threat to pass privacy legislation if Internet firms did not adopt fair information practices in due course: "Because the market for consumer purchasing, demographic, and Web-surfing information was in full swing with a seemingly unlimited future, firms with strong online presences overwhelmingly preferred self-regulation to mandatory privacy standards that might hinder further growth. It was therefore in the interest of the major online firms to encourage smaller firms to adopt privacy practices that satisfied the FTC.").

78. Fed. Trade Comm'n: Fair Information Practice Principles, http://www.ftc.gov/ reports/privacy3/fairinfo.htm (last visited Jan. 31, 2007). The four FIPP include Notice and Awareness, Choice and Consent, Access and Participation, and Security and Integrity. *Id.* Of these, "the FTC considers notice of privacy practices to be the most fundamental, but the law does not compel such notice or mandate the terms of the privacy policy." Nehf, *supra* note 6, at 44.

79. Websites may earn a privacy "seal of approval" from an entity such as TRUSTe (www.truste.org), the Council of Better Business Bureaus (www.bbbonline.org), the

websites not to use advertisers unless they have strong privacy policies,[80] and the development of a "Safe Harbor" agreement with the European Union, whereby U.S. companies wanting to use personal information about EU citizens in the U.S. must recognize more stringent EU prohibitions against using such data.[81]

B. State Law

State law too mandates online privacy policies[82] without governing

---

American Institute of Certified Public Accountants, WebTrust (www.cpawebtrust.org), or the Entertainment Software Rating Board (www.esrb.org/privacy), by conforming to certain guidelines. *See Business Roundtable Report*, *supra* note 27, at 15 ("The primary self-regulatory enforcement initiatives are the online seal programs which require 'licensees' to implement fair information practices and to submit to various types of compliance monitoring to display a privacy seal on their Web sites. . . . According to the FTC, the online seal programs have not yet established a significant presence on the Web.").

80. Several firms have announced they would no longer advertise or link to websites that do not publish privacy practices conforming to fair information practices. *See* Nehf, *supra* note 6, at 3. (citing Jon G. Auerbach, *To Get IBM Ad, Sites Must Post Privacy Policies*, WALL ST. J., Mar. 31, 1999, at B1); *see also* Steven Hetcher, *The De Facto Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109, 118 (2000).

81. *See* Duncan H. Brown & Jeffrey L. Blevins, *The Safe-Harbor Agreement Between the United States & Europe: A Missed Opportunity to Balance the Interests of E-commerce and Privacy Online?*, 46 J. OF BROADCASTING & ELECTRONIC MEDIA 4 (2002).

82. California law now requires all operators of commercial websites or online services that collect personally identifiable information about California consumers to post a privacy policy. Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE § 22575 (West Supp. 2007). Absent some kind of prohibition against use by California residents, websites in all states must now choose either to post a general privacy policy or to take the cumbersome step of posting a separate privacy notice directed only to California residents. *See id.* Because the geographical location of the operator is irrelevant, California's law implicates any website unless the website operator wants to go through the trouble of finding out where the consumer resides before agreeing to collect any information. *See* Sarah B. Kemble, *Privacy Policies: Is There Really a Choice Anymore?* 16 S. CAROLINA LAW. 26 (2004). *But see* RAYMOND T. NIMMER, 1 INFORMATION LAW § 8.90 (West 1996) (questioning constitutionality of California law under the interstate commerce clause).

Other state laws require certain entities like governmental agencies to post privacy policies. For instance, South Carolina's Family Privacy Protection Act requires the posting of privacy policies by any state entity "which hosts, supports, or provides a link to page or site accessible through the world wide web." S.C. CODE ANN. § 30-2-40 (West Supp. 2005). *See also* ARIZ. REV. STAT. ANN. §§ 41-4151-52 (2004 & Supp. 2006); ARK. CODE ANN. § 25-1-114 (Supp. 2005); CAL. GOV'T CODE § 11019.9 (West 2005); COLO. REV. STAT. §§ 24-72-501-02 (2006); DEL. CODE ANN. tit. 29, §§ 9017C-9018C (2006); 5 ILL. COMP. STAT. 177/10(b)(2) (West 2005); IOWA CODE ANN. § 22.11 (West 2001); ME. REV. STAT. ANN. tit. 1, §§ 541-42 (Supp. 2006); MD. CODE ANN., STATE GOV'T § 10-624(c)(4) (LexisNexis 2004); MICH. COMP. LAWS SERV. § 205.827 (LexisNexis Supp. 2006); MINN. STAT. ANN. § 13.15 (West 2005); MONT. CODE ANN. §§ 2-17-550-53 (2005); N.Y. STATE TECH. LAW §§ 201-07 (2006); TEX. GOV'T CODE ANN. § 2054.126 (Vernon Supp. 2006); VA. CODE ANN. §§ 2.2-3800-03 (2005).

the substance of those policies.[83] And like federal law, state law regulates deceptive or false statements in privacy policies.[84] In addition, an increasing number of states are passing legislation requiring businesses to inform residents if their unencrypted personal information has been compromised.[85] Similarly, a number of general application statutes and common law claims have been interpreted to prevent websites from defrauding consumers or violating their privacy statements, but few provide claims for mistreatment of personal information in the absence of some deception or unkept promise.[86]

---

83. California's law requires disclosure of privacy practices and access to personal information, but does not regulate how the website might treat that information if it in fact discloses that treatment. Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE § 22575 (West Supp. 2007). The session law implementing the Act noted that it was "the intent of the Legislature to require each operator of a commercial Web site or online service to provide individual consumers residing in California who use or visit the commercial Web site or online service with notice of its privacy policies, thus improving the knowledge these individuals have as to whether personally identifiable information obtained by the commercial Web site through the Internet may be disclosed, sold, or shared." 2003 Cal. Stat. 829 § 2(b). Other state laws require security provisions but do not otherwise govern use of personal information. For example, Michigan requires any person who obtains one or more social security numbers in the ordinary course of business to create a privacy policy that provides security and prevents access. MICH. COMP. LAWS SERV. § 445.84 (LexisNexis 2006).

84. New York applies its statute, N.Y. GEN. BUS. LAW § 349 (McKinney 2004), which prohibits deceptive practices and false advertising, to a website's privacy promises. *See* Fed. Trade Comm'n v. Crescent Publ'g Group, Inc., 129 F. Supp. 2d 311, 319 (S.D.N.Y. 2001). Pennsylvania makes it illegal for a collector of personal information to knowingly make a false or misleading statement in a published privacy policy about how it will use that information. 18 PA. CONS. STAT. ANN. § 4107 (West Supp. 2006).

85. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501 (West Supp. 2006); ARK. CODE ANN. §§ 4-110-105 (Supp. 2005); CAL. CIV. CODE §§ 1798.29 (West Supp. 2006); COLO. REV. STAT. § 6-1-716 (2006); CONN. GEN. STAT. ANN. §§ 36a-701; 36a-701a; 36a-701b (West Supp. 2006); DEL. CODE ANN. tit. 6, §§ 12B-101-04 (2005); FLA. STAT. § 817.568 (West 2006); GA. CODE ANN. § 10-1-910 (West Supp. 2006); HAW. REV. STAT. § 487N-2 (2006); 815 ILL. COMP. STAT. 530/12 (2006); IND. CODE ANN. § 4-1-11-5 (LexisNexis Supp. 2006); LA. REV. STAT ANN. § 51:3074 (Supp. 2007); ME. REV. STAT. ANN. tit. 10, § 1348 (Supp. 2006); MINN. STAT. ANN. §325E.61 (West Supp. 2006); MONT. CODE ANN. § 31-3-115 (2005); NEV. REV. STAT. ANN. § 603A.220 (LexisNexis Supp. 2006); N.H. REV. STAT. ANN. § 359-C:20 (LexisNexis Supp. 2006); N.J. STAT. ANN. § 56:8-163 (West Supp. 2006); N.Y. GEN. BUS. LAW § 899-aa (McKinney Supp. 2007); N.C. GEN. STAT. § 75-65 (2005); N.D. CENT. CODE § 51-30-02 (Supp. 2005); OHIO REV. CODE ANN. §§ 1347.12; 1349.19 (West Supp. 2006); 73 PA. STAT. ANN. § 2303 (West Supp. 2006); R.I. GEN. LAWS § 11-49.2-3 (Supp. 2006); TENN. CODE ANN. § 47-18-2107 (Supp. 2006); TEX. BUS. & COM. CODE ANN. § 48.103 (Vernon Supp. 2007); WASH. REV. CODE § 19.255.010 (West Supp. 2006). For a discussion of these laws and a list that is periodically updated, *see State PIRG Summary of State Security Freeze and Security Breach Notification Laws*, The State PIRG Consumer Protection Inside Pages, http://www.pirg.org/consumer/credit/statelaws.htm (lasted visited Jan. 31, 2007).

86. Some states have general application statutes prohibiting "invasion of privacy" or "intrusion upon seclusion" that may be asserted in a variety of situations where

C. *Government Enforcement*

Consistent with the focus on disclosure rather than substance, most enforcement with respect to the treatment of personal information has been in the form of FTC enforcement actions brought against website companies who violated the terms of their own privacy policies.[87] As of August 2006, the FTC had brought actions resulting in eighteen consent agreements or stipulated judgments[88] pursuant to the Unfair Trade Practices Statute (Section 5 of the FTC Act),[89] five actions[90] under the Fair Credit Reporting Act,[91] and eleven actions[92] pursuant to the

---

consumers' information is unexpectedly or unreasonably used, sold or shared. *See* Hill v. MCI Worldcom Commc'ns, Inc., 141 F. Supp. 2d 1205, 1209 (S.D. Iowa 2001) (disclosure of phone numbers and addresses of consumer's friends to a stalker was cognizable as invasion of privacy); Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003) (finding that Docusearch.com, an investigation service, may be held liable for negligence or invasion of privacy for selling personal information to a client over the Internet, where that client used the information to track and murder New Hampshire resident Amy Boyer); McGuire v. Shubert, 722 A.2d 1087, 1090 (Pa. Super. Ct. 1998) (a customer whose bank account information has been disclosed by the bank to a third party may have a cause of action for invasion of privacy).

87. The few actions brought against companies that did not involve misrepresentations in privacy policies allege that the company failed to provide adequate security for personal information stored online, in violation of Section 5 of the FTC Act. *See In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465, 2005 FTC LEXIS 134 (2005); *In re* CardSystems Solutions, Inc., 2005 FTC LEXIS 176 (2005); *In re* DSW Inc., 70 Fed. Reg. 73,474 (Fed. Trade Comm'n Dec. 12, 2005) (analysis of proposed consent order). For example, in the action against BJ's Wholesale Club, a warehouse membership chain of stores, the FTC alleged that the company stored members' personal information on computers and failed to employ reasonable and appropriate security measures to protect it, resulting in several million dollars' worth of fraudulent purchases made with counterfeit copies of members' credit and debit cards. *In re* BJ's Wholesale Club, Inc., 2005 FTC LEXIS 140, at *4 (2005).

88. *See, e.g.*, United States v. ChoicePoint Inc., No. 1:06-CV-0198 (N.D. Ga. Jan. 30, 2006); Fed. Trade Comm'n v. ToySmart.com, LLC, No. Civ.A. 00-CV11341RGS, 2000 WL 1523287 (D. Mass. Aug. 21, 2000); DSW Inc., 70 Fed. Reg. at 73,474; CardSystems Solutions, Inc. 71 Fed. Reg. 10,686 (Fed. Trade Comm'n March 2, 2006) (analysis of proposed consent order); *In* re *BJ's Wholesale Club, Inc.*, 2005 FTC LEXIS 134, at *1; *In re* Petco Animal Supplies, Inc., 139 F.T.C. 102, 113, 2005 FTC LEXIS 40 (2005); *In re* Vision I Props., LLC, 139 F.T.C. 296, 302; 2005 FTC LEXIS 66 (2005); *In re* Gateway Learning Corp., 2004 FTC LEXIS 150, at *10 (2004); *In re* MTS, Inc. d/b/a Tower Records/Books/Video, 2004 FTC LEXIS 88, at *8 (2004); *In re* Educ. Research Ctr. of Am., Inc., 2003 FTC LEXIS 72, at *10 (2003); *In re* Guess?, Inc., 2003 FTC LEXIS 123, at *10 (2003); *In re* Nat'l Research Ctr. for Coll. & Univ. Admissions, Inc., 2003 FTC LEXIS 9, at *10 (2003); *In re* Eli Lilly & Co., 2002 FTC LEXIS 22, at *9 (2002); *In re* Microsoft Corp. 2002 FTC LEXIS 43, at *11 (2002); *In re* GeoCities, 127 F.T.C. 94, 1999 FTC LEXIS 17, at *11 (1999); *In re* Liberty Fin. Cos., 1999 FTC LEXIS 46, at *5 (1999).

89. *See* 15 U.S.C.A. § 45(a) (West 1997).

90. *See, e.g.*, *In re* Quicken Loans Inc., 2002 FTC LEXIS 96, at *6 (2002); *In re* First Am. Real Estate Solutions, LLC, 1998 FTC LEXIS 115, at *5 (1998).

91. *See* 15 U.S.C.A. § 1681 (West 1998).

Children's Online Privacy Protection Act ("COPPA").[93]

Other enforcement actions have been brought by the FTC for failure to provide adequate security of online personal information in violation of websites' own representations that the information would be treated in a secure and safe manner, a violation of Section 5 of the FTC Act.[94]

And a number of enforcement actions have been brought against companies for sharing, renting, or selling personal information in violation of promises in online privacy policies, but only where there is such a promise.[95]

State attorneys general have brought enforcement actions under the state statutory equivalents of the federal unfair/deceptive practices act that focus primarily on failure to abide by privacy policy terms. Recently, New York's Attorney General Elliot Spitzer brought an action against Gratis Internet Inc., alleging that the Internet company sold the personal information of approximately seven million people who used its websites, breaching its privacy promises.[96] Spitzer called the case "the

92. *See, e.g.*, United States v. Hershey Foods Corp., Civ. No. 4:03-cv-00350-JEJ (M.D. Pa. Feb. 26, 2003); United States v. Mrs. Fields Famous Brands, Civ. No. 2:03cv00205 (D. Utah Feb. 25, 2003); United States v. Ohio Art Co., Civ. No. 3:02CV7203 (N.D. Ohio Apr. 30, 2002); United States v. Am. Pop Corn Co., Civ. No. C02-4008DEO (N.D. Iowa Feb. 28, 2002); United States v. Lisa Frank, Inc., Civ. No. 01-1516-A (E.D. Va. Oct. 3, 2001); United States v. Looksmart, Ltd., Civ. No. 01-606-A (E.D. Va. Apr. 23, 2001); United States v. Bigmailbox.com, Inc., Civ. No. 01-605-A (E.D. Va. Apr. 23, 2001); United States v. Monarch Servs., Inc., Civ. No. AMD 01 CV 1165 (D. Md. Apr. 20, 2001); *In re* Bonzi Software, Inc., 2004 FTC LEXIS 206, at *10 (2004).

93. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C.A. § 6501 (West Supp. 2006).

94. *See* United States v. ChoicePoint Inc., No. 1:06-CV-0198 (N.D. Ga. Jan. 30, 2006); *In re* Petco Animal Supplies, Inc., 2005 FTC LEXIS 40, at *1; *In re* MTS, Inc. d/b/a Tower Records/Books/Video, 2004 FTC LEXIS 88, at *8; *In re Guess?, Inc.*, 2003 FTC LEXIS 123, at *10; *In re* Eli *Lilly & Co.*, 2002 FTC LEXIS 22, at *9; *In re Microsoft Corp.*, 2002 FTC LEXIS 43, at *11.

95. *See* Fed. Trade Comm'n v. ToySmart.com, LLC, No. Civ.A. 00-CV11341RGS, 2000 WL 1523287 (D. Mass. Aug. 21, 2000) (bankrupt retail toystore offered customer lists for sale in violation of privacy policy); *In re Vision I Props., LLC*, 139 F.T.C. at 302 (retail merchants who use CartManager often had privacy policies saying they would not share personal information, but CartManager rented that information); *In re Gateway Learning Corp.*, 2004 FTC LEXIS 150, at *10 (educational products company rented personal information provided online despite privacy statements to the contrary); *In re Educ. Research Ctr. of Am., Inc.*, 2003 FTC LEXIS 72, at *10 (companies' marketing materials and privacy statements stated that survey information collected offline from school students would only be shared with educational entities, but information was in fact shared with third party marketers for commercial purposes); *In re GeoCities*, 1999 FTC LEXIS 17, at *11 (online privacy statements misrepresented purposes for collecting personal information and that information would not be disclosed to third parties without permission).

96. *See* New York v. Gratis Internet, Inc. No. 401210/06, 2006 WL 777061 (N.Y. Sup. Ct. Super. Ct. March 22, 2006).

largest deliberate breach of a privacy policy ever discovered by U.S. law enforcement."[97] According to the complaint, from 2000 to 2004, Gratis operated six websites through which consumers could obtain free products.[98] Privacy policies on those sites stated that Gratis would never sell, lend or loan personal information submitted by users of the sites, and specifically promised not to share email addresses.[99] Nonetheless, during 2004 and 2005 Gratis allegedly sold personal information it had collected to three other firms.[100]

New York's Attorney General has also brought recent actions against Yahoo!,[101] Victoria's Secret,[102] and Chase Manhattan Bank[103] based on failure to comply with online privacy promises.[104] Yahoo! promised its customers that submitted to its privacy policy that it would not share telephone numbers, but then announced that its privacy policy was being amended to allow sharing of such numbers.[105] After the state investigation, Yahoo! agreed not to share the numbers or misuse them.[106]

---

97. *Web Firm Sold Info of 7 Million People, New York Suit Claims*, 23 No. 22 ANDREWS COMPUTER & INTERNET LITIG. REP. 11 (Apr. 4, 2006).

98. *Gratis Internet*, 2006 WL 777061.

99. *Id.*

100. *Id.*

101. Kenneth M. Dreifach, *Data Privacy, Web Security, & Attorney General Enforcement*, 865 PLI/PAT 355, 369 (2006).

102. *Id.* at 371.

103. *Id.* at 373.

104. *See also* Don Tellock, Assistant Attorney General, Internet Bureau, Office of the New York State Attorney General, Remarks at the Consumer Reports WebWatch's First National Summit on Web Credibility: Scams & Schemes: Why Don't Consumers Trust the Web? (April 24, 2003), *available at* http://64.78.25.46/dynamic/conferences-summit2003-why-dont-consumers-trust.cfm (stating that the American Civil Liberties Union experienced security breach of personal information obtained from its online store customers despite the website's privacy promises); Toys R Us.com Enters into Agreement with State, Jan. 3, 2002, http://www.state.nj.us/lps/ca/press/toysrus.htm (stating that ToysRUs.com entered into agreement with the New Jersey Attorney General settling a dispute as to personally identifiable information collected from online purchasers and agreeing to change its privacy policy to avoid misrepresentations); Kenneth M. Dreifach, *supra* note 102, at 372-73 (noting that ten states investigated DoubleClick's collection and analysis of users' personal information and surfing habits). The DoubleClick investigation was prompted by DoubleClick's proposed merger with Abacus, another marketer, and by DoubleClick's own public promises about its privacy practices. *Id.* at 372. It focused on how the company discloses its practice of assigning anonymous but unique "cookie" identifiers to the computers of web surfing consumers. *Id.* DoubleClick collected consumer data during its display of web-page banner ads and used cookies to track the surfing activity of any given computer across a wide network of website clients. *Id.* The Assurance required that websites allowing DoubleClick to profile its visitors must disclose DoubleClick's activities through a privacy policy, DoubleClick must protect that information, post its own clear and conspicuous privacy policy and permit customers to opt-in to an email alert service describing amendments to its privacy, submit to audits, and pay a $450,000 fine to the states. *Id.* at 372-73.

105. *Id.* at 369.

106. *Id.*

Victoria's Secret was found to have exaggerated the level of privacy and security given its customers' personal information when, contrary to its promises that data would remain "in private files" and that the site provided "stringent and effective security measures," personal data was in fact accessible through web files.[107] Chase Manhattan Bank agreed to clarify its privacy policy and cease sharing customers' account and credit information with non-affiliated third-party marketers despite its broad promises that "safeguarding [personal customer] information is a matter we take very seriously" and that it only shared information for security reasons or to "make available special products."[108]

Thus the focus of FTC and state enforcement is primarily on the website's adherence to its promises, not a general standard of fairness. If the website follows its own policy and provides reasonable security, it is free to do what it wants with a user's personal information.[109]

D. Private Enforcement

Private actions too have been unsuccessful in curtailing websites' use of personal information in the absence of a broken promise. Besides the enforcement actions discussed above, case law regarding websites' adherence to their privacy policies is still sparse. The majority of private actions have arisen out of the provision of passenger personal information by airlines to entities studying security issues in the wake of September 11. In those cases, the airlines defended against passengers' claims that the disclosure constituted a violation of their privacy policy by arguing that the policies were not binding.[110]

In *In re American Airlines, Inc., Privacy Litigation*,[111] plaintiffs alleged that American Airlines, Inc. ("American") violated its website's privacy policy when American disclosed passenger information to the Transportation Security Administration ("TSA"). The court dismissed the passengers' breach of contract claim based on American's violation of its promise not to disclose that information because the passengers

107. *Id.* at 371.

108. *Id.* at 373; *cf.* Smith v. Chase Manhattan Bank, 741 N.Y.S.2d 100 (N.Y. App. Div. 2002) (parallel private litigation where the court granted dismissal based on failure of the complaint to allege specific instances of "actual harm").

109. *See* Chris Jay Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment*, ELEC. PRIVACY INFO. CTR ., March 4, 2005, http://www.epic.org/reports/decadedisappoint.pdf (noting that self-regulation "certainly is the least intrusive approach for companies exploiting personal information, but it has not efficiently ensured Fair Information Practices" but of the five Fair Information Practices, "only notice can be said to be present as a result of privacy statements").

110. The policies at issue did not contain the contractual language that is more common in such policies today. *See supra* Part II.

111. 370 F. Supp. 2d 552 (N.D. Tex. 2005).

failed to allege damages.[112] The court also dismissed claims based on Section 2701 of the Wiretap Act because American authorized the third party data collector, Airline Automation, Inc., to disclose the passenger information to the TSA.[113] Furthermore, the court dismissed the ECPA Section 2702 claim because of the statutory exception for disclosure with "the lawful consent of... an... intended recipient of such communication" (i.e., Airline Automation).[114] The disclosure admittedly violated American's privacy policy, but a breach of contract is not "unlawful" in a criminal sense, which is required by the ECPA.[115]

In *In re Northwest Airlines Privacy Litigation*,[116] the court denied recovery to classes of plaintiffs/passengers who alleged that, post 9/11, Northwest Airlines ("Northwest") had breached its privacy policy by providing the National Aeronautics and Space Administration with passenger names, flight numbers, credit card information, hotel and car rental reservations and traveling companions' names.[117] The court dismissed the plaintiffs' breach of contract claim, finding that the admittedly-unread privacy policy was a general statement of company policy rather than a contract.[118] The court also found that the plaintiffs failed to allege any contract damages.[119] In addition, the court dismissed the plaintiffs' claims under the ECPA, finding no improper access to electronic communication service provider information under section 2701, and that Northwest was not an electronic communication service provider under section 2702.[120]

Similarly, in *In re Jetblue Airways Corp. Privacy Litigation*,[121] plaintiff passengers brought a class action for violation of their privacy rights arising out of JetBlue's transfer of passenger personal information to Defendant Torch Concepts, Inc. for use in a federally-funded study on military base security.[122] The court found claims under New York's

112. *Id.* at 567.
113. *Id.* at 558-59.
114. *Id.* at 561.
115. *Id.* at 560 (citation omitted).
116. No. Civ.04-126(PAM/JSM), 2004 WL 1278459, at *6 (D. Minn. June 6, 2004).
117. *Id.* at *1, *6.
118. *Id.* at *6.
119. *Id.*
120. *Id.* at *2. *See also* Dyer v. Northwest Airlines Corps., 334 F. Supp. 2d 1196 (D.N.D. 2004). In *Dyer*, the plaintiff's ECPA section 2702 claim was dismissed because Northwest is not an electronic communications service provider and the breach of contract claim was dismissed because it was based on a privacy policy and the court found it a policy, not a contract. *See id.* at 1200. The plaintiffs made no allegation that they logged onto a website or read a privacy policy and made no allegation of damages. *Id.*
121. 379 F. Supp. 2d 299 (E.D.N.Y. 2005).
122. *See id.* at 303.

General Business Law and other state consumer protection statutes to be preempted by the ADA.[123] The plaintiffs' breach of contract claims based on JetBlue's privacy policy were dismissed because of a failure to allege actual damages;[124] failure to allege they read the policy was not, however, a ground for dismissal.[125] Plaintiffs' ECPA section 2702 claim was dismissed because JetBlue is not an electronic communications service provider.[126]

In at least one private enforcement action, a website's privacy policy provided some insulation against identity theft claims *because* the policy did not "guarantee" against identity theft.[127] In *Kuhn v. Capital One Financial Corp.*, online customers brought a putative class action alleging that Capital One failed to respond adequately to a security breach of a retail website server, resulting in loss of customer information.[128] Plaintiffs' claims included breach of contract based on the online privacy policy.[129] The court found no misrepresentations in the bank's privacy policy, which included "no guarantee against illicit use" of customer information,[130] and instead the policy "openly acknowledge[d] the possibility of identity theft and ma[de] no guarantees against its occurrence."[131]

The only other private actions concerning privacy policies to date involve the use of third party data collectors, and in those cases the privacy policies potentially exempt the website companies from liability for certain use of personal information because the substantive legislation excepts "authorized" use of the information.[132] In *Crowley v.*

123. *Id.* at 324.

124. *See id.* at 327.

125. *See id.* at 325-26.

126. *See id.* at 310; *see also* Privacy Rights Clearinghouse v. Jetblue Airways Corp., No. D045568, 2005 WL 3118798, at *1 (Cal. Ct. App. Nov. 22, 2005) (affirming decision that claims based on unfair business practices arising out of failure to abide by privacy policy were preempted by the ADA; breach of contract itself not preempted, but not at issue because claim was not brought by passengers themselves).

127. *See* Kuhn v. Capital One Fin. Corp., No. CA015177, 2004 WL 3090707, at *3 (Mass. Super. Nov. 30, 2004).

128. *See id.* at *1.

129. *See id.* at *3.

130. *Id.* at *3.

131. *Id.*

132. In a twist, one such case upheld a claim by the website based on consumers' violations of its privacy policy by failing to accurately and truthfully complete their Subscriber Profiles and failing to accept the commercial email received by them in a proper manner. *See* Gordon v. Impulse Mktg. Group, Inc., No. CV-04-5125-FVS, 2006 WL 624838, at *3-4 (E.D. Wash. Mar. 9, 2006) (upholding claim by Internet marketing company against third party defendants who submitted subscriber profiles and entered into privacy policies seeking to direct email to the plaintiff website and base a suit against the website for violation of consumer protection statutes regarding unsolicited email).

Cybersource Corp.,[133] a customer of Amazon's retail website brought a purported class action against Amazon.com and its third-party verification company, Cybersource Corp., alleging that Cybersource stored customer information in violation of the Wiretap Act and the ECPA.[134] The plaintiff also brought a claim for breach of contract against Amazon. The court dismissed the Wiretap Act claim, finding that Amazon did not "intercept" an electronic communication from its customer by simply receiving an email from the customer,[135] and dismissed the ECPA claim because Amazon is not an electronic communication provider under that statute,[136] and its access to plaintiff's communications was not "unauthorized."[137]

In *In re Pharmatrak, Inc. Privacy Litigation*,[138] customers of several pharmaceutical companies brought a class action against those companies and Pharmatrak (with whom the companies had a contractual relationship) based on personal information gathered by Pharmatrak from the companies' websites using cookies. The court reversed the dismissal of ECPA claims against Pharmatrak, finding that the pharmaceutical companies did not consent to Pharmatrak's collection of personal information from customers.[139] Had Pharmatrak consented to the companies' interception, its customers would have had no claim against those companies.[140] And had Pharmatrak's privacy policy with its own customers allowed the information gathering, Pharmatrak too would have had authorization for any such information gathering.[141]

In none of these actions did the privacy policy provide any protection to the consumers that they would not have had absent the policy. And in a few cases, the policy actually gave the website company greater leeway to use personal information, because the statute at issue had an exception for consent or authorization by a party to the communication.

---

133. 166 F. Supp. 2d 1263 (N.D. Cal. 2001).

134. *See id.* at 1265.

135. *Id.* at 1269.

136. *Id.* at 1270.

137. *Id.* at 1271-72. The court declined to exercise supplemental jurisdiction over the plaintiff's state law claims, including breach of contract. *Id.* at 1272-73.

138. 329 F.3d 9, 19-20 (1st Cir. 2003).

139. *Id.* at 20.

140. *See id.* at 20-21.

141. *See id.* at 21-22. Indeed, many privacy policies disclose that the website company uses cookies to gather information automatically about visitors, even without the visitors being aware that such information is gathered. *See* Amazon.com Privacy Policy, *supra* note 40; Yahoo! Mail Privacy Center, http://privacy.yahoo.com/privacy/us/mail/ (last visited Jan. 31, 2007) (disclosing that the website receives and stores information from visitors automatically via cookies).

IV. Privacy Policies and the Online Visitor—The Disconnect

The end-result of ubiquitous privacy policies should be an increase in the actual privacy of consumers' personal information. However, scholars note that the result of the disclosure approach that has developed seems instead to be the exact opposite: more "the appearance of privacy" than the reality.[142]

The self-governance model has been criticized as privacy policies proliferate but privacy protection wanes.[143] David A. DeMarco observes that "under self-regulation, the principles of notice/awareness and choice/consent are unequivocally (and unsurprisingly) skewed in favor of business interests."[144] Joseph Turow opines, based on a national survey

---

142. Nehf, *supra* note 6, at 3-4.

> [P]rivacy policies can be seen everywhere today, and they give the impression that Web sites safeguard personal information that they collect. When the policies are read, however, there is often very little privacy protection being promised. Policies might disclose how data is collected and how it will be transferred, sold, or traded, but often the message is that information will be collected in whatever way the Web site can obtain it, and the site reserves the right to share or sell it with impunity. References to information security or safeguards tend to be vague and noncommittal. Thus, despite the proliferation of privacy policies online, consumers' privacy interests may in fact be no better protected today than they were ten years ago.

Id. (footnotes omitted); *see also* Solove & Hoofnagle, *supra* note 21, at 357 (opining that current U.S. privacy law does not adequately address the activities of the database industry, and suggesting certain changes in legislation, including universal notice of all companies collecting personal information, ensuring meaningful informed consent about the uses and dissemination of PI, the ability of consumers to manage their credit records and ensure the accuracy of their PI, and various security measures); Katherine J. Strandburg, *Privacy, Rationality & Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1286 (2005).

> Consumers as a whole might be better off penalizing sites that do not offer a high level of privacy protection by refusing to deal with them, but for each individual consumer it is rational to attempt to free ride on the boycott efforts of others. Consumers are unable to enforce a boycott because they cannot detect and penalize defectors. This analysis suggests that consumers will not be able to sustain a 'norm against tempters' that penalizes such websites.

Id. (footnotes omitted); Richard Warner, *Surveillance & the Self: Privacy, Identity, & Technology*, 54 DEPAUL L. REV. 847, 848 (2005) (arguing that "[t]o ensure sufficient power [to control what others can learn about us and what they can do with what they learn], businesses should be required to obtain our consent before they collect certain types of information about us," and that "the 'consent requirement' is insufficient on its own to protect privacy adequately," so additional statutory protection is necessary).

143. *See* Nehf, *supra* note 6, at 3-4.

> The FTC lauded the success of its market-driven solution. The FTC placed its faith in market incentives to curb unfair privacy practices, but there may be little incentive for online businesses to adopt and adhere to strong privacy policies. *It is the appearance of privacy that seems to matter most.*

Id. (footnotes omitted) (emphasis added).

144. David A. DeMarco, Note, *Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood & Pragmatism, Pop-tarts & Six-packs*, 84

of adults who use the Internet at home, that "years into attempts by governments and advocacy groups to educate people about Internet privacy, the system is more broken than ever."[145] And Chris Hoofnagle reports that "[w]e now have ten years of experience with privacy self-regulation online, and the evidence points to a sustained failure of business to provide reasonable privacy protections."[146]

The danger lies in the fact that consumers believe they have more privacy simply because of the proliferation of privacy policies. One survey found that 75% of consumers believed that just because a site has a privacy policy, it is not allowed to sell to others the personal information customers disclosed to it.[147] More recently, 57% believed that the mere presence of a privacy policy meant that the website could not share consumers' personal information with other websites or companies.[148] In fact, a survey in 2000 found that 83% of website privacy policies allow the site to share personal information with third parties.[149] Consumer misapprehension about the effect of privacy policies is not surprising considering the evidence that few ever read the policies, and even if they did, might not understand the data practices being disclosed.[150]

The solutions proposed by privacy advocates range from substantive legislation to conform privacy practices to the FTC's Fair Information Practices;[151] to "patience" while "market influences such as advertising,

---

TEX. L. REV. 1013, 1047 (2006) (stating that Amazon.com's privacy policy "gives only vague notice regarding how it uses information and offers only a very limited extent of control—basically an all-or-nothing choice—over how submitted personal information can be used").

145. TUROW, *supra* note 53, at 3.

146. Hoofnagle, *supra* note 110, at 1.

147. JOSEPH TUROW, LAUREN FELDMAN & KIMBERLY MELTZER, OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE, A REPORT FROM THE ANNENBERG PUBLIC POLICY CENTER OF THE UNIVERSITY OF PENNSYLVANIA 3 (2005).

148. TUROW, *supra* note 53, at 4.

149. Miyazaki & Fernandez, *supra* note 1, at 58 (finding only 17% of websites surveyed disclosed that they would *not* share personal information with third parties).

150. *See* DeMarco, *supra* note 145, at 1047 ("[S]ince there are few legal restraints on what the company can do with information once the information is in its hands and since customers are not very demanding with regard to the ways in which their information may be utilized, it makes good business sense to keep the policy as vague as possible."); Nehf, *supra* note 6, at 43 n.220 (noting that after the passage of federal legislation like the GLBA and HIPAA, "legions of lawyers" have become involved in drafting privacy policies that are lengthier and more difficult to understand than even before); TUROW, *supra* note 53, at 9-10 (discussing "world of legalistically phrased privacy policies" that are long, ambiguous, and hard to read).

151. In March 2005, the Electronic Privacy Information Center ("EPIC") issued a study arguing that after "ten years of experience with privacy self-regulation online, and the evidence points to a sustained failure of business to provide reasonable privacy protections." Hoofnagle, *supra* note 110, at 1. EPIC calls upon the FTC and Congress "to create a floor of standards for protection of personal information based on Fair

personal experience, privacy signals (such as privacy trust marks), and technological developments[152] make privacy terms more salient;"[153] to encouraging more government enforcement.[154]

In the meantime, there is a distinct possibility that as website operators grow savvier with respect to the law, they will respond to the lack of substantive privacy protection (and lack of consumer awareness) by including in privacy policies terms that are not favorable to consumers.[155] Thus, operators will make the cost-benefit calculation that allowing themselves the option of sharing such information in their privacy policies will outweigh any risk that such a provision will prevent consumers from sharing their information in the first place.[156] At the

---

Information Practices." *Id.* Daniel Solove and Chris Hoofnagle have proposed a Model Privacy Regime to address problems in United States privacy protection, aiming "to patch up the holes in existing privacy regulation and improve and extend it." Solove & Hoofnagle, *supra* note 21, at 357. Solove and Hoofnagle suggest sixteen methods in which the Fair Information Practices advocated by the FTC in its self-regulation approach should instead by incorporated into specific legislation. *Id.*

152. Technological solutions include software options like the Platform for Privacy Preferences ("P3P"), which is an industry-promoted software solution to online privacy concerns that allows consumers to choose what information they wish to share with websites and for what purposes. When a site seeks additional information or wants to use the information for other purposes, the user's browser displays a warning. *See* Kimberly Rose Goldberg, Note, *Platform for Privacy Preferences ("P3P"): Finding Consumer Assent to Electronic Privacy Policies*, 14 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 255, 256 (2003).

153. Nehf, *supra* note 6, at 5-6.

154. The FTC and state attorneys general have used their unfair trade practices statutes to target online companies that violate their privacy policies, or that negligently fail to provide adequate security to consumers' personal information. These agencies could broaden the scope of that enforcement to include privacy practices whereby a website obtains a consumer's information for one purpose and later uses it for another, or unreasonably shares or sells such information. The problem here is that websites' privacy policies are increasingly likely to give them that very ability. The FTC is unlikely to find any practice "unfair" that is specifically allowed by the privacy policy. As Professor Nehf noted, "The FTC will declare a practice unfair only if the injury is not one that consumers can reasonably avoid. The FTC views its role as promoting consumer choice, not second-guessing those choices. It will not change market outcomes when the injury can be avoided by consumers taking reasonable actions themselves." *Id.* at 46 (citations omitted). However, the FTC has brought actions against firms that "take advantage of poorly informed decision making," suggesting that consumers may be able to challenge the idea that they could have "reasonably avoided" the privacy injury. *Id.* at 50. As Professor Nehf pointed out, consumers may argue that it would be unreasonable to require that they read a privacy policy, understand its implications, and take protective action. *Id.*

155. Researchers have found that, by using certain techniques in framing and wording of questions, website operators can almost guarantee a "yes" answer. *Public Opinion on Privacy*, ELEC. PRIVACY INFO. CTR., http://www.epic.org/privacy/survey/ (last visited Jan. 31, 2007) ("Using the right combination of question framing and default answer, an online organization can almost guarantee it will get the consent [for information collection] of nearly every visitor to its site.").

156. *See* Hildebrand & Klosek, *supra* note 7, at 20-21 (advising companies to craft

least, such policies will continue to include other non-consumer-friendly terms like arbitration or forum selection clauses.[157]

While an online visitor is not likely to bring suit against a website company for rescission of a privacy policy based on the fact that it gives the company the ability to sell or share visitor information,[158] a visitor may well find itself in a position to challenge the policy as not binding if faced with a privacy dispute against the website.[159] If so, how can the consumer challenge the policy's enforceability?

V. Challenging Enforcement

A. Lack of Assent

The most obvious challenge to the enforceability of an online privacy policy as a binding contract is that the website visitor failed to assent to the agreement. A contract is only enforceable if both parties have manifested their assent to its terms.[160]

An analogy can be made to the online license agreement, about which there is a large body of case law discussing online contract formation.[161] Those cases have found that users are bound to online

---

their privacy policies to allow themselves the flexibility to share data with third parties).

157. *See supra* Part II.

158. First, the visitor is usually unaware of the policy, much less that any increase in unsolicited email or risk of identity theft is due to the particular website's sharing of information. Second, as discussed above, without the breach of a privacy policy there is little substantive law to prevent the sale or sharing of personal information. Finally, there are many practical problems with a law suit based on a website's sharing of personal information, including the requirement that the visitor prove damages. *See infra* notes 188-90 and accompanying text.

159. For example, AOL customers recently brought suit against that company based on AOL's disclosure of customers' search requests. *Subscribers Sue AOL Over Data Breach*, CNNMONEY.COM, Sept. 26, 2006, http://money.cnn.com/2006/09/26/technology/aol_suit/index.htm. A broad reading of its privacy policy could potentially lend the company a defense against those claims. Similarly, a government entity could bring an enforcement action against a company for violation of the Wiretap Act or ECPA, and challenge the company's use of the privacy policy as "authorization" under the exceptions to those statutes.

160. E. ALLEN FARNSWORTH, CONTRACTS § 3.1 (4th ed. 2004).

161. *See, e.g.*, Register.com v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004) (finding assent to online registrar agreement despite the fact that the terms of the agreement did not appear until after the user submitted its query and received data; while plaintiff's argument may have prevailed for the first such search, the user here had submitted numerous queries daily, and was aware of the restrictions on its use); ProCD, Inc. v. Zeidenburg, 86 F.3d 1447 (7th Cir. 1996); Specht v. Netscape, 150 F. Supp. 2d 585, 594 (S.D.N.Y. 2001) (no assent to online license agreement where "user is not required to click on an icon expressing assent to the license, or even view its terms, before proceeding to use the information on the site").

licenses to which they have "clicked" acceptance[162] or where they have actual notice of the terms.[163] One colorful description of "clickwrap" comes from the District of Massachusetts:

> Has this happened to you? You plunk down a pretty penny for the latest and greatest software, speed back to your computer, tear open the box, shove the CD-ROM into the computer, click on "install" and, after scrolling past a license agreement which would take at least fifteen minutes to read, find yourself staring at the following dialog box: "I agree." Do you click on the box? You probably do not agree in your heart of hearts, but you click anyway, not about to let some pesky legalese delay the moment for which you've been waiting. Is that "clickwrap" license agreement enforceable? Yes, at least in the case described below.[164]

Users are not bound to license agreements that are only visible to the user by "browsing"—scrolling down the screen or to a different screen—and where the user is not required to view the license in order to complete the transaction.[165]

In *Davidson & Assoc. v. Internet Gateway*,[166] the plaintiff alleged that the defendants breached its license agreement and Terms of Use when the defendants used reverse engineering to learn plaintiff's computer games protocol and distribute rival software. The court upheld the enforceability of the online contracts based on their clickwrap formation requirement; the online user had to click "I Agree" to the

---

162. I.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2005) (finding assent to online license agreement where computer software required user to click assent to the agreement before continuing with installation); *see also* DeJohn v. TV Corp. Int'l, 245 F. Supp. 2d 913 (N.D. Ill. 2003) (upholding clickwrap services agreement of domain name registration service); Hughes v. McMenamon, 204 F. Supp. 2d 178 (D. Mass. 2002) (upholding clickwrap member agreement between subscriber and Internet service provider); Net2Phone, Inc. v. Super. Ct., 135 Cal Rpt. 2d 149 (Cal. Ct. App. 2003) (upholding clickwrap terms of use); Forrest v. Verizon Commc'ns, Inc., 805 A.2d 1007 (D.C. 2002) (upholding 13-page clickwrap Internet services agreement); Caspi v. Microsoft Corp., 732 A.2d 528 (N.J. Super. Ct. 1999) (upholding clickwrap online subscriber agreement); Groff v. America Online, Inc., 1998 R.I. Super. LEXIS 46 (1998) (upholding forum selection clause in online subscriber agreement that required clicked acceptance); Barnett v. Network Solutions, Inc., 38 S.W.3d 200 (Tex. Ct. App. 2001) (upholding online clickwrap domain name registration agreement, which required user to scroll through and accept or reject the agreement).

163. *Register.com*, 356 F.3d at 401; Cairo, Inc. v. Crossmedia Servs., Inc., No. C. 04-04825 JW, 2005 WL 756610 (N.D. Cal. Apr. 1, 2005) (repeated and automated use of a website can form the basis of implied notice of the user of the website services' terms).

164. *I. Lan Systems*, 183 F. Supp. 2d at 329.

165. *See Specht*, 150 F. Supp. 2d at 594. Even a browsewrap agreement will be upheld where the user has actual knowledge of the agreement. *See Register.com*, 356 F.3d at 403.

166. 334 F. Supp. 2d 1164 (E.D. Mo. 2004).

terms of the license to proceed with installation of the software.[167]

In *Motise v. America Online, Inc.*,[168] the court rejected AOL's argument that its forum selection clause was binding upon the plaintiff, a non-subscriber who was using another's AOL service, regardless of whether he had actual notice of it because "his status as a user of AOL's services gave him constructive notice" of the clause. Instead, the court found that Second Circuit precedent required that contract terms "appear on the screen, in view of the user, for the user to be on notice of them."[169]

Similarly, in *Defontes v. Dell Computers Corp.*,[170] the court found no manifestation of assent to online terms and conditions that were only accessible via an inconspicuous hyperlink at the bottom of the Dell Computer's web page.[171]

The fact that the online agreement requires a user to click acceptance might not be sufficient if the user is not required to view a link to that agreement for his application to be processed. In *Comb v. Paypal Inc.*,[172] the court declined to uphold a lengthy online user agreement where the user could have completed the application process without ever viewing the user agreement and arbitration clause. And in *Strujan v. AOL*,[173] the court declined to uphold the forum selection clause in AOL's Member Terms of Service Agreement, where the user was not required to read each page.[174] Finally, in *Williams v. America Online, Inc.*,[175] the court declined to uphold AOL's forum selection clause where the agreement's terms were accessible only by twice overriding the default choice of "I Agree" and clicking "Read Now" twice.

In the one case squarely considering the question of whether an online privacy policy was enforceable as a contract, it was the website company who argued that the policy was not a contract. In *In re Northwest Airlines Privacy Litigation*,[176] plaintiff customers of the airline argued that its provision of their personal information to the National Aeronautical and Space Administration ("NASA") to assist NASA in studying ways to increase airline security violated Northwest's privacy

167. *Id.*

168. 346 F. Supp. 2d 563 (S.D.N.Y. 2004).

169. *Id.* at 565 (citing *Specht*, 306 F.3d at 20). The court nonetheless granted AOL's motion to transfer on the basis that the plaintiff was a sublicensee of an AOL user who had accepted the terms of service.

170. No. C.A. PC 03-2636, 2004 WL 253560 (R.I. Super. Ct. Jan. 29, 2004).

171. *Id.* at *6.

172. 218 F. Supp. 2d 1165 (N.D. Cal. 2002).

173. No. 055175/05, 2006 WL 1452778 (N.Y. Civ. Ct. May 19, 2006).

174. *Id.* at *1. The court was most concerned with the fact that the forum selection clause would prevent the plaintiff from taking advantage of New York City's Civil Court procedures, which were designed to accommodate unrepresented persons. *Id.* at *2.

175. No. 00-0962, 2001 WL 135825 (Mass. Super. Ct. Feb. 8, 2001).

176. No. Civ. 04-126(PAM/JSM), 2004 WL 1278459 (D. Minn. June 6, 2004).

policy, which stated that Northwest would not share customers' information except as necessary to make their travel arrangements.[177] In addition to dismissing the plaintiffs' federal statutory claims, the court agreed with Northwest's argument that plaintiffs' breach of contract and warranty claims should be dismissed because the privacy policy did not constitute a unilateral contract:[178]

> The usual rule in contract cases is that "general statements of policy are not contractual." ... The privacy statement on Northwest's website did not constitute a unilateral contract. The language used vests discretion in Northwest to determine when the information is "relevant" and which "third parties" might need that information. Moreover, absent an allegation that Plaintiffs actually read the privacy policy, not merely the general allegation that Plaintiffs' "relied on" the policy, Plaintiffs have failed to allege an essential element of a contract claim: that the alleged "offer" was accepted by Plaintiffs.[179]

The district court in *Dyer v. Northwest Airlines Corp.*[180] agreed with the "policy, not contract" conclusion. There, a class action arising out of the same disclosure of passenger information to the NASA, the court agreed with Northwest that its online privacy policy was not a contract. With little analysis, the court found, "broad statements of company policy do not generally give rise to contract claims."[181] The court also stated that the breach of contract claim failed because "nowhere in the complaint are the Plaintiffs alleged to have ever logged onto Northwest Airlines' website and accessed, read, understood, actually relied upon, or otherwise considered Northwest Airlines' privacy policy."[182] These decisions have been criticized by commentators[183] and disagreed with by

177. Northwest's website privacy policy stated: "When you reserve or purchase travel services through Northwest Airlines nwa.com Reservations, we provide only the relevant information required by the car rental agency, hotel, or other involved third party to ensure the successful fulfillment of your travel arrangements." *Id.* at *5-6.

178. Presumably, the court discussed the policy in terms of a unilateral rather than a bilateral contract because its terms would provide for a promise on the part of Northwest (not to share information) in exchange for an act on the part of the customer (providing information). *See* FARNSWORTH, *supra* note 161, at § 3.4 (unilateral contracts formed by promise in exchange for performance).

179. *In re Northwest Airlines Privacy Litig.*, 2004 WL 1278459, at *6. The court also granted the motion to dismiss the contract claim based on plaintiffs' failure to allege damages. *Id.*

180. Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004).

181. *Id.* at 1200.

182. *Id.*

183. Moringiello & Reynolds, *supra* note 52, at 446 ("[The] statement [in *In re Northwest*] is clearly inconsistent with hornbook contract law. . . .").

courts.[184]

In contrast, in *In re JetBlue Corp. Privacy Litigation*,[185] the court found the failure to allege that the plaintiffs read the privacy policy was not fatal to their breach of contract claims, and that the allegation of reliance was sufficient.[186] However, the court granted dismissal of the breach of contract claims based on failure to allege damages.[187] Similarly, in *In re American Airlines, Inc. Privacy Litigation*,[188] the court dismissed without prejudice plaintiffs' breach of contract claims based on failure to allege damages, not failure to allege the existence of a contract.[189]

As discussed above, privacy policies are often presented in terms of browsewrap.[190] Users are deemed to have agreed to them simply by being on the website or by disclosing information on the site. Rather than being required to click on the privacy policy, the agreements are usually presented as inconspicuous hyperlinks at the bottom of a screen. These users have a strong argument under existing precedent that they were not given adequate notice of the policies and did not assent to them.[191]

Similarly, many websites "invite" users to view their policy rather than requiring the user to read it and agree to it before providing any personal information to the website.

Assent to the amendment of privacy policies is also likely to be

---

184. *See In re* JetBlue Corp. Privacy Litig., 379 F. Supp. 2d 299, 325 (E.D.N.Y. 2005) (the holding in *In re Northwest* that the plaintiffs' failure to read the policy or otherwise allege acceptance of its terms defeated their contract claim "rest[s] on an overly narrow reading of the pleadings"); Schafer v. AT&T Wireless, No. Civ. 04-4149-JLF, 2005 WL 850459, at *4-5 (S.D. Ill. April 1, 2005) (a contract need not be read for its terms to be effective).

185. 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

186. *Id.* at 325-26.

187. *Id.* at 327.

188. 370 F. Supp. 2d 552 (N.D. Tex. 2005).

189. *Id.* at 567.

190. *See supra* Part II.

191. One additional reason why privacy policies may fail to bind consumers is a result of their tendency to "invite" rather than require the user to view the policy. In Specht v. Netscape Commc'ns Corp., 150 F. Supp. 2d 585, 596 (S.D.N.Y. 2001) (footnote omitted), the court noted that the individual obtaining Netscape's SmartDownload software is not made aware that he is entering into a contract:

> Couched in the mild request, "Please review [and agree to the terms of the license agreement before downloading]," this language reads as a mere invitation, not as a condition. The language does not indicate that a user *must* agree to the license terms before downloading and using the software. While clearer language appears in the License Agreement itself, the language of the invitation does not require the reading of those terms or provide adequate notice either that a contract is being created or that the terms of the License Agreement will bind the user.

challengeable.[192] Many website companies purport to retain the right to amend privacy policies with or without notice to the consumers from whom they have received personal information.[193] Gateway Learning Corporation collected customer information pursuant to explicit promises in its privacy policy that it would not sell, share, or rent that information.[194] Subsequently, Gateway changed its privacy policy to allow sharing of previously-received personal information with notice or consent. The FTC brought an action against Gateway for misrepresentation and unfair and deceptive practices.[195]

Thus, particularly in cases where consumers are deemed to have assented to privacy policies by virtue of their presence on the site or by giving information without affirmatively clicking acceptance, the consumer has a good argument that he or she did not assent to the privacy policy, preventing the formation of a binding contract, and preventing the website from enforcing any of its terms against the consumer. Purported amendments that apply automatically without requiring assent are similarly open to challenge.

B. Unconscionability

Second, a consumer might make an unconscionability argument to avoid enforcement of certain terms of an online privacy policy. The doctrine of unconscionability is a judicial tool for policing unfair contracts.[196] Its emergence can be linked to the growing use of typical

192. In addition, amendment via email notice without the requirement of a responsive email is also likely to be found insufficient. In Campbell v. Gen. Dynamics Gov't Sys. Corp., 407 F.3d 546 (1st Cir. 2005), the defendant attempted to amend an employment contract via email to include an arbitration clause. The mass email stated that the new policy was to be effective beginning the following day, and did not require any response from the employees. The court found this method insufficient to bind the email recipients:

> One way that General Dynamics could have set this particular communication apart from the crowd would have been to require a response to the email. Instead, the company opted for a "no response required" format. . . . Signing an acknowledgement or, in a more modern context, clicking a box on a computer screen, are acts associated with entering into contracts. Requiring an affirmative response of that sort would have signaled that the Policy was contractual in nature.

Id. at 556-57.

193. *See supra* Part II.

194. *In re* Gateway Learning Corp., 2004 FTC LEXIS 150, at *10 (2004).

195. *Id.* Similarly, Yahoo! purported to amend its privacy policy, announcing that telephone numbers submitted with the understanding that they would not be shared would not be shared. Attorney General of the State of New York, Internet Bureau, *In re Yahoo! Inc.*, Assurance of Discontinuance (Sep. 24, 2003), *available at* http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/nys/nyagyahoo92403aod.pdf. After New York's Attorney General investigated, the company agreed not to share the numbers or misuse them. *Id.*

196. *See* CHARLES L.KNAPP, NATHAN M. CRYSTAL & HARRY G. PRINCE, PROBLEMS IN

standard form contracts with boilerplate provisions.[197] The doctrine is codified in the Uniform Commercial Code[198] and incorporated in the Restatement (Second) of Contracts,[199] and has been used by courts to police unfairness or one-sidedness in a variety of contract terms.[200] Most states require a showing both of procedural and substantive unconscionability in order to refuse enforcement of a contract term.[201]

1. Procedural Unconscionability

Procedural unconscionability focuses on the process in which the parties enter into the contract.[202] Hallmarks of procedural unconscionability include unequal bargaining positions, undue length, fine print, confusing language, and misleading terms.[203] Importantly, even if procedural issues in connection with the consumer's acceptance of the online privacy policy are not extreme enough to convince a court that the consumer failed to assent to the contract, they may be sufficient to rise to the level of procedural unconscionability.

Some courts find the procedural unconscionability element satisfied

---

CONTRACT LAW 667-669 (Aspen Law & Business 4th ed. 1999).

197. *Id.* at 668.

198. U.C.C § 2-302 (2004). While the UCC would not apply to a transaction purely of personal information (which is not a good), its authority is persuasive. Moreover, where personal information is provided as part of the purchase of a good, the UCC might be deemed to govern the entire transaction.

199. RESTATEMENT (SECOND) OF CONTRACTS § 208 (1981).

200. *See* Circuit City Stores, Inc. v. Adams, 279 F.3d 889 (9th Cir. 2002) (finding unconscionable mandatory arbitration provision in employment contract that bound employees only); Williams v. Walker-Thomas Furniture Co., 350 F.2d 445 (D.C. Cir. 1965) (invalidating consumer retail installment contract that provided that each item purchased became security for the payment for all items purchased); Green v. Cont'l Rentals, 678 A.2d 759 (N.J. Super. Ct. Law Div. 1994) (excessive interest charged in rent-to-own contracts rendered terms unconscionable); Art's Flower Shop v. Chesapeake & Potomac Tel. Co., 413 S.E.2d 670 (W. Va. 1991) (refusing to enforce limitation of liability clause from omission of advertisement where telephone company had monopoly over yellow pages directory).

201. *See Williams*, 350 F.2d at 449 ("Unconscionability has generally been recognized to include an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party."); Davidson & Assocs., Inc. v. Internet Gateway, Inc., 334 F. Supp. 2d 1164, 1179 (E.D. Mo. 2004); Am. Stone Diamond, Inc. v. Lloyds of London, 934 F. Supp. 839, 844 (S.D. Tex. 1996); Dean Witter Reynolds, Inc. v. Super. Ct., 259 Cal. Rptr. 789, 795 (Cal. Ct. App. 1989).

202. *See Davidson & Assocs., Inc.*, 334 F. Supp. 2d 1164, 1179 (E.D. Mo. 2004) ("Procedural unconscionability concerns the manner in which the contract was negotiated and the circumstances of the parties at the time.").

203. *See Williams*, 350 F.2d at 449 ("Did each party to the contract, considering his obvious education or lack of it, have a reasonable opportunity to understand the terms of the contract, or were the important terms hidden in a maze of fine print and minimized by deceptive sales practices?").

simply by a showing that the agreement at issue is one of adhesion.[204] A contract of adhesion is a standard form agreement offered on a take-it or leave-it basis.[205] The online context is uniquely suited to adhesive agreements, as website visitors have no real ability to bargain. To combine terms, online contracts are very often "click-it" or leave-it. Online privacy policies are no exception.[206]

2. Substantive Unconscionability

The second prong of the unconscionability argument focuses on the one-sidedness or unfairness of terms.[207] Contract terms that have been found to be unreasonably favorable to one side include extreme price terms[208] and limitation of remedies.[209]

In addition, there is ample authority for refusing to enforce one-sided arbitration clauses.[210] For example, in *Comb v. Paypal, Inc.*,[211] the

204. *See* Comb v. Paypal, Inc., 218 F. Supp. 2d 1165, 1172 (N.D. Cal. 2002).

205. *See* Kristian v. Comcast Corp., 446 F.3d 25, 32 n.2 (1st Cir. 2006).

206. Some websites do provide phone numbers for consumers to call if they do not agree with privacy terms, but this seems, again, to be more form than substance—while consumers might opt out of sharing their information with certain third parties, there is no evidence that consumers are ever able to negotiate arbitration or forum selection clauses. *See* Nehf, *supra* note 6, at 8 n.33 ("Drafters of some adhesion contracts, particularly end-user license agreements for software, may attempt at least to give the appearance of negotiable terms (and thereby deflect potential unconscionability claims) by including a telephone number that the licensee can call if terms are not satisfactory or if additional rights are desired.").

207. *See* FARNSWORTH, *supra* note 161, at 300-303.

208. *See* Perdue v. Crocker Nat'l Bank, 702 P.2d 503 (Cal. 1985).

209. *See* U.C.C. §§ 2-719(3) (2004) (clauses limiting or excluding liability for consequential damages).

210. *See* Circuit City Stores, Inc. v. Adams, 279 F.3d 889 (9th Cir. 2002) (arbitration agreement requiring that employees arbitrate their claims against employer without imposing reciprocal requirement upon employer, together with limitations on employees' potential relief, found unconscionably one-sided); Ticknor v. Choice Hotels Int'l, Inc., 265 F.3d 931, 939-40 (9th Cir. 2001) (under Montana law, arbitration clause requiring franchisee to arbitrate its claims against hotel chain, but allowing hotel chain access to courts, was unconscionable); Armendariz v. Found. Health Psychcare Servs., Inc., 6 P.3d 669 (Cal. 2000) (arbitration provision unconscionable where it required that employees arbitrate their claims against employer but not vice versa and limited damages recoverable by employee but not employer); Bellsouth Mobility LLC v. Christopher, 819 So. 2d 171 (Fla. Dist. Ct. App. 2002) (language of contract clause supported lower court's determination of substantive unconscionability because it limits Bellsouth's liability to actual damages irrespective of its level of culpability, precluded class action relief, and allowed Bellsouth but not its customer the option of suit in court; remanding for evidentiary hearing on procedural unconscionability issue); Iwen v. U.S. W. Direct, Inc., 977 P.2d 989 (Mont. 1999) (arbitration agreement between telecommunications company and yellow page advertiser unconscionable where only the advertiser was bound to arbitrate its claims); Burch v. Second Judicial Dist. Ct., 49 P.3d 647 (Nev. 2002) (arbitration clause substantively unconscionable where it grants housing developer exclusive right to choose arbitrators and rules governing the arbitration); O'Donoghue v.

court denied the website company's motion to compel arbitration, finding substantive unconscionability where the user agreement allowed PayPal, in the event of a dispute, "'at its sole discretion' [to] restrict accounts, withhold funds, undertake its own investigation of a customer's financial records, close accounts, and procure ownership of all funds in dispute unless and until the customer is 'later determined to be entitled to the funds in dispute.'"[212] This provision, along with the fact that PayPal alone made the final decision with respect to a dispute and maintained the right to change the user agreement without prior notice, resulted in a lack of mutuality of remedies.[213]

Also important in rendering the PayPal clause substantively unconscionable was the fact that it expressly prohibited PayPal customers from consolidating their claims. This, coupled with the costs the plaintiff would have to bear, rendered a dispute prohibitively expensive for a single litigant:

> By allowing for prohibitive arbitration fees and precluding joinder of claims (which would make each individual customer's participation in arbitration more economical), PayPal appears to be attempting to insulate itself contractually from any meaningful challenge to its alleged practices. Under these circumstances, the Court concludes that this aspect of the arbitration clause is so harsh as to be substantively unconscionable.[214]

Similarly, in *Defontes v. Dell Computers Corp.*,[215] the court found an arbitration clause substantively unconscionable because its language was so one-sided as to render it an unenforceable illusory promise. The arbitration clause specified that any claim "against Dell" arising out of the customer's relationship with Dell must be submitted to arbitration, and it stated that the terms and conditions were subject to change at any time without prior notice, in Dell's sole discretion.[216]

In addition to challenging arbitration clauses or the enforceability of a provision allowing the website company to change the privacy policy

---

Smythe, Cramer Co., No. 80453, 2002 WL 1454074, at *5 (Ohio Ct. App. July 3, 2002) (arbitration clause in home purchase contract unconscionable where plaintiff's filing fee would exceed maximum recovery under contract's limitation of liability); State *ex rel.* Dunlap v. Berger, 567 S.E.2d 265 (W. Va. 2002) (arbitration agreement unconscionable where it prohibited punitive damages regardless of level of retailer's wrongdoing and denied class action relief, both of which would otherwise be available in consumer fraud action).

211. 218 F. Supp. 2d 1165 (N.D. Cal. 2002).
212. *Id.* at 1173-74.
213. *Id.*
214. *Id.* at 1176.
215. No. C.A. PC 03-2636, 2004 WL 253560 (R.I. Super. Jan. 29, 2004).
216. *Id.*

at any time without notice, a consumer may attempt to challenge as unconscionable other privacy terms that are inconsistent with the FTC fair information practices, such as an inability to access personal information or control its use.[217]

C. *Challenging Forum Selection Clauses*

As with arbitration clauses, privacy policies often include a forum selection clause or incorporate by reference such a clause in the website's general terms and conditions. In contrast to an arbitration clause, a forum selection clause usually specifies a particular state in which a claim must be brought, rather than requiring the waiver of the right to a jury trial or other rights under the court system.[218] Simply because such a clause is included in the terms and conditions does not mean that it will apply to claims based on the website privacy policy, unless the privacy policy incorporates the forum selection clause.[219]

The standards applied by courts in refusing enforcement of forum selection clauses are lower than those applied to arbitration clauses. A forum selection clause may be held invalid simply for being "unreasonable or unjust."[220]

There has been considerable litigation recently over the forum selection clause included in participation agreements by online companies such as America Online and Verizon requiring that any suit be brought in the state courts of Virginia. Importantly, the state courts of

---

217. *See supra* note 79 (discussing Fair Information Practice); *but see* Moringiello & Reynolds, *supra* note 52, at 435 (courts focus on whether the buyer had reasonable notice of the online terms restricting their rights, but do not question whether those terms are substantively fair).

218. Black's Dictionary defines "forum selection clause" as "[a] contractual provision in which the parties establish the place (such as the country, state, or type of court) for specified litigation between them." BLACK'S LAW DICTIONARY 681 (8th ed. 2004).

219. *See* Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263 (N.D. Cal. 2001) (forum selection clause contained in online retailer's participation agreement did not apply to claims that the retailer violated its privacy policy; privacy policy was referenced in the participation agreement but not incorporated).

220. *See* Forrest v. Verizon Commc'ns, Inc., 805 A.2d 1007, 1010-11 (D.C. 2002) (forum selection clause not "unreasonable under the circumstances" even though required forum would not permit class action procedure); America Online, Inc. v. Booker, 781 So. 2d 423 (Fla. Dist. Ct. App. 2001) (forum selection clause in terms of use was not unreasonable or unjust); Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999) (online subscriber agreement requiring suit to be brought in state of Washington upheld; forum selection clause did not fit within any of New Jersey's three exceptions to enforceability); Groff v. America Online, Inc., No. PC 97-0331, 1998 WL 307001 (R.I. Super. May 28, 1998) (forum selection clause not unreasonable); Barnett v. Network Solutions, Inc., 38 S.W.3d 200, 202 (Tex. App. 2001) (forum selection clause in online domain registration agreement not "fundamentally unfair and unenforceable").

Virginia do not permit class action procedures.[221] Courts in Florida,[222] Texas,[223] the District of Columbia,[224] Rhode Island,[225] the District of Massachusetts[226] and the Southern District of New York[227] have upheld such forum selection clauses, while state and local courts in New York[228] and Massachusetts[229] have struck them down.

The arguments that have been successful in challenging such forum selection clauses are that the clause was not readily accessible to the online customer,[230] or that the designated forum will effectively deny the plaintiff a legal remedy.[231] Thus, a forum selection clause in a privacy policy may be struck down both for formation problems and for failing to provide a forum that is convenient to the plaintiff or that would allow him the remedies of his chosen forum.

VI. Conclusion

Not all websites are required to have privacy policies, but most of them do—and for good reason. Existing legislation and case law allow the website to insulate itself from any controls on its use of personal information by providing disclosure, as they focus on whether a website has truthfully revealed what it may in fact do with its customers' personal information. The websites do not appear to face any real threat of losing business by revealing that they may share or even sell such information, despite consumers' concerns about online privacy, because consumers rarely read, much less understand, online privacy policies.

In addition to allowing the sites the freedom to do what they wish with personal information, those policies often include other terms that are unfavorable to consumers. While a change in the law to provide substantive privacy protections is the best solution, it does not appear to

221. *Booker*, 781 So. 2d at 424 ("[T]here is no mechanism for class actions in Virginia state courts. . . .").

222. *See id.* at 425.

223. *See Barnett*, 38 S.W.3d at 203-04.

224. *See Forrest*, 805 A.2d at 1013.

225. *See Groff*, 1998 WL 307001 at *4-5.

226. *See* Hughes v. McMenamon, 204 F. Supp. 2d 178, 181 (D. Mass. 2002).

227. *See* Motise v. America Online, Inc., 346 F. Supp. 2d 563, 566 (S.D.N.Y. 2004).

228. *See* Strujan v. AOL, No. 055175/05, 2006 WL 1452778 (N.Y. Civ. Ct. May 19, 2006); Scarcella v. America Online, Inc., 811 N.Y.S.2d 858 (N.Y App. Div. 2005).

229. *See* Williams v. America Online, Inc., No. 00-0962, 2001 WL 135825 (Mass. Super. Feb. 8, 2001).

230. *Id.* at *1 (forum-selection clause requiring suit to be brought in VA not upheld where agreement terms accessible only by twice overriding default choice of "I Agree" and clicking "Read Now" twice).

231. *See Strujan*, 2006 WL 1452778, at *1 (forum selection clause not reasonable in light of public policy embodied in personal appearance provisions designed to accommodate unrepresented persons in plaintiff's chosen forum); *Scarcella*, 811 N.Y.S.2d at 858 (forum selection clause not reasonable in context of small claims case).

be on the horizon. Therefore, if a privacy issue does arise that is arguably governed by the website's privacy policy, consumers are likely in the future to want to challenge—not enforce—the policy's binding effect. Their best arguments for doing so are (1) a lack of assent, as many online privacy policies still employ browsewrap acceptance features; and (2) unconscionability of terms like arbitration clauses or unreasonability of forum selection clauses. Rather than providing consumers the protection they expect, privacy policies have become one more online contract of adhesion for consumers to avoid.