Online Privacy Policies: Contracting Away Control Over Personal Information?

Allyson W Haynes

Available at: https://works.bepress.com/allyson_haynes/1/
Online Privacy Policies: Contracting Away Control Over Personal Information?

Allyson W. Haynes*

Table of Contents

I. Introduction ................................................................................................................. 587
II. Privacy Policies and the Online Trade in Personal Information ......................... 590
   A. Online Provision of Personal Information ....................................................... 590
   B. Privacy Policy Terms ....................................................................................... 593
      1. Use of Personal Information ........................................................................ 594
      2. Dispute Resolution and Other Terms ............................................................... 595
      3. Binding Nature of the Policy and Amendments Thereto .............................. 596
II. Privacy Policies and the Law .................................................................................... 597
   A. Federal Law ....................................................................................................... 598
   B. State Law .......................................................................................................... 601
   C. Government Enforcement .................................................................................. 603
   D. Private Enforcement ......................................................................................... 606
III. Privacy Policies and the Online Visitor—The Disconnect .................................... 610
IV. Challenging Enforcement ....................................................................................... 613
   A. Lack of Assent ................................................................................................... 613
   B. Unconscionability ............................................................................................. 618
      1. Procedural Unconscionability ....................................................................... 619
      2. Substantive Unconscionability ...................................................................... 620
   C. Challenging Forum Selection Clauses ................................................................. 622
V. Conclusion ................................................................................................................. 623

I. Introduction

In the process of making an online purchase from “Webo,” 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 Webo 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.
incentive of a website operator to disclose the potential for broad use of personal information, even if such use is not currently contemplated.\footnote{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 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 intersection 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,\footnote{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/ stanford/7L.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," Neff 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.I. Culnan & G.R. Millo, The Culnan-Milloy Survey of Consumers and Online Privacy Notices: Summary of Responses 1, 2 (2001), http://www.fcc.gov/cgb/workshop/privacy/supporting/culnan-milloy.pdf consumers still do not seem to read online privacy policies); Humphrey Taylor, Most People Are "Privacy Pragmatists." Who, Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits, THE HARRIS POLL NO. 17, March 19, 2003, http://www.harristeenativeinteractive.com/harris_poll/index.aspx?PID=665.

7. See Mary J. Hildebrand & Jacqueline Klock, Recent Security Breaches Highlight the Important Role of Data Security in Privacy Compliance Programs, 17 INT’L. PROP. & TECH. J.L., 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. Neff, 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," 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 is provided by website visitors in numerous ways. From the simple act of providing an email address for the purpose of receiving an email newsletter, the provision of a credit card number and mailing address to facilitate a purchase, to the most risky provision of social security numbers and other financial information to a bank in order to apply for a loan, personal information is given freely and often in the ever-growing online American market.

There is growing attention to the security that websites afford such personal information 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; AOL's recent disclosure of search data entered by more than 650,000 subscribers; and the security breach at LexisNexis resulting in improper access to personal information belonging to about 310,000 people. 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.

References:
10. The term "personal information" is used here as it is defined under federal law: (i) individually identifiable information about an individual collected online, including—(A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.


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. § 2721(3) (West 2000) ("personal 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."

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


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


14. In 2005, total e-commerce sales in the United States were estimated at $863 billion, an increase of 25.6% 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/retailsat/www/data/mkt/05Q4.html.

15. There has also been increased attention to the threat of online sexual predators, particularly those who target children. See Chelsea Kelner, 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.eyewitnessnews.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).

16. 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 655,000 members of the Reserves—had been stolen in what has become "one of the nation's largest security breaches")

17. See Saul Hansell, AOL Removes Search Data on Fast 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).


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, as well as contribute to the less perennial, but thoroughly irritating and often expensive, increase in spam.

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 1999 to an overwhelming 88% of 1,500 Internet users being very or somewhat concerned about websites’ collection of personal information in 2003. The issue of personal information privacy even promises to be a factor in the 2008 presidential election. 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 and as a voluntary measure by websites to appeal to consumers by emphasizing the care with which they treat consumer information. In 1998, only 2% of all websites had some form of privacy notice, and in 1999, eighteen of the top 100 shopping sites did not display a privacy policy. By 2001, virtually all of the most popular commercial websites had privacy notices, with the number continuing to increase through 2005.

25. Cf. Clinton Touts Privacy Bill of Rights, NEWSDAY, June 16, 2006, at A16 (“[S]enate Democrats may add a privacy deed to the bill” and in the House “privacy protection measures are being inserted ‘to meet the need’”). See also THE NATION (June 16, 2006) (reporting that “there is a strong movement to make online privacy an issue in the election”).

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://www2.brookings.edu/programs/01/041101.pdf (noting that businesses may provide privacy policies as a voluntary measure to protect consumer privacy); also see Hillebrand & Kloas, 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 online privacy policies.”).

28. See Neih, 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.”).


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. 2, 22 (2001) (statement of Timothy J. Morris, 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.”).

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

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 ("While 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 churchers post a great deal of personal information online, less than 3% of church websites post a privacy policy. Marisa 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 (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 e-mail. See generally Spam: Unsolicited Commercial E-mail. ELIC, PRIVACY BLOG, CTY. http://www.epic.org/privacy/junk_mail/spam (last visited Jan. 31, 2007); SURFER REVIEW, supra note 30.
38. Via hyperlink, users are told “[t]he AOL Network’s affiliated providers include, 2007] ONLINE PRIVACY POLICIES 595

“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.39 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.
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 “by 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 TRANSMIT 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 Unfair 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 B.U. LAW. 433, 444 (2005) (discussing Union Fédérée des Consommateurs Que Choisir v. AOL, T.G.I. Nanterre, J.C.P. 2004 II, 10022, note Pages).

2007] ONLINE PRIVACY POLICIES 597
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/confid/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/bmu/about/disclaimer.asp (the “Terms of Use”).”.
54. USA TODAY.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 online 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.48

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,”49 protects “customer proprietary network information” from disclosure by telecommunications carriers,50 regulates how federal governmental agencies gather and handle personal data,51 and requires financial services companies to implement measures to protect the security and confidentiality of their customers’ personal information.52 In addition, legislation restricts the use and disclosure of certain specific types of personal information, including individually identifiable health information,53 education records,54 and consumer reports.55

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.56

58. See supra Part III.A (discussing legislative exceptions). Commentators have observed that 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) (“[W]ith 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.”).


...
the statute.\footnote{75} In the past, there has been a push by the federal government to regulate the use of websites' treatment of personal information in addition to requiring that certain entities disclose that treatment.\footnote{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."\footnote{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.

Other aspects of the so-called self-governance model of U.S. privacy policy include privacy seals of approval,\footnote{78} voluntary pledges by websites not to use advertisers unless they have strong privacy policies,\footnote{79} 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.\footnote{80} According to the FTC, the online seal programs have not yet established a significant presence on the Web.

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 Neff, supra note 6, at 3. (citing Jan G. Auerbach, To Get IBM All, Sites Must Post Privacy Policies, WALL ST. J., MAR. 31, 1999, at B11); see also Steven Hetchler, The De Facto Federal Privacy Commission, 19 J. MARSHALL J. COMPUTER & INFO. L. 257 (2002).


78. 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 2001, 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. CALIFORNIA LAW, 26 (2004). But see TEMPEST N. NIMMER, 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 a page or site accessible through the world wide web." S.C. CODE ANN. §§ 36-2-40 (West Supp. 2005). See also ARIZ. REV. STAT. ANN. §§ 41-4151-52 (2004 & Supp. 2006); ARK. CODE ANN. § 25-5-114 (Supp. 2005); CAL. GOV'T CODE § 11019.9 (West 2005); COLO. REV. STAT. §§ 24-70-91, 24-70-92 (2006); D.C. CODE ANN. ¶ 30-531 (2006); ILL. COMP. STAT. ANN. 1055/1 (2007); IOWA CODE ANN. § 52.12 (2003); ME. REV. STAT. ANN. tit. 1, §§ 541-42 (Supp. 2006); MD. CODE ANN., STATE GOV'T § 10-624(b)(4) (Lexis/Nexis 2004); MICH. COMP. LAWS ANN. § 250.287 (Lexis/Nexis Supp. 2006); MICH. STAT. ANN. § 13.15 (West 2005); MONT. CODE ANN. §§ 2-17-551 through 2-17-551(13) (2005); N.Y. STATE TECHL. LAW §§ 201-07 (2006); TEX. GOV'T CODE ANN. § 2504.126 (Vernon Supp. 2006); VA. CODE ANN. §§ 2.2-3800-03 (2005).
the substance of those policies. And like federal law, state law regulates deceptive or false statements in privacy policies. In addition, an increasing number of states are passing legislation requiring businesses to inform residents if their unencrypted personal information has been compromised. 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 upkeep promise.

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 Ann § 445.564 (LexisNexis 2006).


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 a consumer’s 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 residents Amy Boyerj, McGain v. Shubert, 722 A.2d 1087, 1090 (Pa. Super. Ct. 1998) (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., 200 F.D.R. 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).


Children’s Online Privacy Protection Act (“COPPA”).92  

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.93

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.94

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 againstGratis Internet Inc., alleging that the Internet company sold the personal information of approximately seven million people who used its websites, breaching its privacy promises.95 Spitzer acted as “the


95. See Fed. Trade Comm’n v. Toymart.com, LLC, No. Civ.A. 00-CV-1314(RGS), 2000 WL 1523328 (D. Mass. Aug. 21, 2000) (bankrupt retailer turned off its online customer lists for sale in violation of privacy policy); In re Vision I Propcs., 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 collected that information); In re Gateway Learning Corp., 2004 FTC LEXIS 150, at *10 (educational products company rented personal information provided online despite privacy promises and the contrary); In re Educa: Research Ctr. of Am., Inc., 2003 FTC LEXIS 72, at *19 (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).


98. Gratis Internet, 2006 WL 777061.

99. Id.

100. Id.

101. Id.

102. Id.

103. Id.

104. Id.

105. 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://78.70.119.11/dynamic/conferencesummit/2003-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 Aciuse, 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 websites. 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 $540,000 fine to the states. Id. at 372-73.

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.\footnote{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."\footnote{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.\footnote{109}

\subsection*{D. Private Enforcement}

Private actions too have been unsuccessful in curtailting 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 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.\footnote{110}

In \textit{In re American Airlines, Inc., Privacy Litigation},\footnote{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 failed to allege damages.\footnote{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.\footnote{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).\footnote{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.\footnote{115}

In \textit{In re Northwest Airlines Privacy Litigation},\footnote{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.\footnote{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.\footnote{118} The court also found that the plaintiffs failed to allege any contract damages.\footnote{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.\footnote{120}

Similarly, in \textit{In re JetBlue Airways Corp. Privacy Litigation},\footnote{121} plaintiffs brought a class action for violation of their privacy rights arising out of JetBlue's transfer of passenger personal information to Defendent Torch Concepts, Inc. for use in a federally-funded study on military base security.\footnote{122} The court found claims under New York's

\footnotesize{\begin{thebibliography}{99}
\item[107.] Id. at 371.
\item[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").
\item[109.] See Chris Jay Hoofnagle, \textit{Privacy Self-Regulation: A Decade of Disappointment}, \textit{ELEC. PRIVACY ENG. CTR.}, March 4, 2005, \texttt{http://www.epic.org/reports/decadedisappointment.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").
\item[110.] The policies at issue did not contain the contractual language that is more common in such policies today. \textit{See supra} Part II.
\item[111.] 370 F. Supp. 2d 552 (N.D. Tex. 2005).
\item[112.] Id. at 567.
\item[113.] Id. at 558-59.
\item[114.] Id. at 561.
\item[115.] Id. at 560 (citation omitted).
\item[117.] Id. at *1, *6.
\item[118.] Id. at *6.
\item[119.] Id.
\item[120.] Id. at *2.
\item[121.] See also Dyer v. Northwest Airlines Corp., 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. \textit{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.
\item[122.] Id. at 379 F. Supp. 2d 299 (E.D.N.Y. 2005).
\item[123.] Id. at 303.
\end{thebibliography}}
General Business Law and other state consumer protection statutes to be preempted by the ADA. The plaintiffs' breach of contract claims based on JetBlue's privacy policy were dismissed because of a failure to allege actual damages; failure to allege they read the policy was not, however, a ground for dismissal. Plaintiffs' ECPA section 2702 claim was dismissed because JetBlue is not an electronic communications service provider.

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. 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. Plaintiffs' claims included breach of contract based on the online privacy policy. The court found no misrepresentations in the bank's privacy policy, which included "no guarantee against illicit use" of customer information, and instead the policy "openly acknowledge[d] the possibility of identity theft and made no guarantees against its occurrence."

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. In Crowley v. Cybersource Corp., 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. 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, and dismissed the ECPA claim because Amazon is not an electronic communication provider under that statute. Its access to plaintiff's communications was not "unauthorized."

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

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.
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. Neff, supra note 6, at 3-4.

143. Privacy 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 standards 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.

144. Id. (footnotes omitted); see also Solove & Hoofnagle, supra note 21, at 357 (arguing 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 tippers that penalizes such websites.

145. See Neff, supra note 6, at 3-4.

The FTC failed 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.

146. 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
personal experience, privacy signals (such as privacy trust marks), and technological developments make privacy terms more salient to encouraging more government enforcement. 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. 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. At the

Information Practices." Id. Daniel Solove and Chris Hoofing 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 & Hoofing, supra note 21, at 557. Solove and Hoofing suggest sixteen methods in which the Fair Information Practices advocated by the FTC in its self-regulation approach should instead be incorporated into specific legislation. Id.

152. Technological solutions include software options like the Platform for Privacy Preferences ("F3P"), 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 ("F3P"): Finding Consumer Assent to Electronic Privacy Policies, 14 FORENSIC INT'LS. PROF. MEDIA & ENT. L.J. 253, 256 (2003).

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

154. The FTC and state attorneys general have used their unfair trade practices statute to target online companies that violate their privacy policies, or that unreasonably 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 has it used 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 action on their own." 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, EPIC 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 & Klossek, supra note 7, at 20-21 (advising companies to craft their privacy policies to allow themselves the flexibility to share data with third parties).
licenses to which they have “clicked” acceptance or where they have actual notice of the terms. 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.

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.

In Davidson & Assoc. v. Internet Gateway, the plaintiff alleged that the defendant breached its license agreement and Terms of Use when the defendant 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 terms of the license to proceed with installation of the software.

In Motise v. America Online, Inc., 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.”

Similarly, in Defontes v. Dell Computers Corp., 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. 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., 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 Straun v. AOL, 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. Finally, in Williams v. America Online, Inc., 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, 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 terms.
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 \textit{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 www.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. \textit{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.


181. Id. at 1200.

182. Id.

183. Moretine & Reynolds, supra note 52, at 446 (“[T]he statement [in \textit{In re Northwest}] is clearly inconsistent with hornbook contract law . . .”).
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 would 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 selecting 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.


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://www.findlaw.com/news.findlaw.com/docs/ny/nyag/yahoo/9243456.pdf. After New York’s Attorney General investigated, the company agreed not to share the numbers or misuse them. Id.

196. See CHARLES L. KRAH & NATHAN M. CRISTAL & 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


197. Id. at 668.

198. U.C.C § 2-202 (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.


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 at the time of contract was to be purchased at retail price); Green v. Court! Court! 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 & Assoc.s, 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 (E.D. Tex. 1996); Dean Witter Reynolds, Inc. v. Super. Ct., 259 Cal. Rptr. 789, 795 (Cal. Ct. App. 1989).

202. See Davidion & Assoc.s, 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. A contract of adhesion is a standard form agreement offered on a take-it-or-leave-it basis. The online contract 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.

2. Substantive Unconscionability

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

In addition, there is ample authority for refusing to enforce one-sided arbitration clauses. For example, in Comb v. PayPal, Inc., the 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." 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.

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.

Similarly, in Defontes v. Dell Computers Corp., 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.

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

205. See Kristine v. Comcast Corp., 446 F.3d 235, 237 (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 Nahl, 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 negotiability (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 Fashionworld, supra note 161, at 306-303.
210. See Circuit City Stores, Inc. v. Adums, 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 951, 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); Arriandtirz v. Found. Health Psychiatric Sys., Inc., 6 P.3d 689 (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 limited 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 issues); 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.
at any time without notice, a consumer may attempt to challenge as unconsolable 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 enforcing forum selection clauses are lower than those applied to arbitration clauses. A forum selection clause may be held invalid simply for being "unreasonable or unfair." 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 Virginia.

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 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).


221. Bubber, 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.


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 Sturijn, 2006 WL 1453778, 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 browswrap 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.