July, 2008

Web Site Visitors and Online Privacy: What Have You Agreed to Share?

Allyson W Haynes


COOKIES

Web Site Visitors and Online Privacy

What Have You Agreed to Share?

By Allyson W. Haynes

Introduction

Imagine that while making an online purchase from a retail Web site, you disclose certain personal information, including your e-mail address. Soon thereafter, you receive an onslaught of unsolicited e-mails from advertisers seeking your business. Has the Web site company violated the law by sharing or even selling your e-mail address? If you want to sue the Web site, can you do so in the forum of your choice? The answer might lie not in state or even federal legislation, but in a contract that you unwittingly entered when you made the online purchase. You might have agreed not only that the Web site can share your personal information, but that if any dispute arises concerning the use of that information, you must arbitrate or sue in a particular state's courts. Unbeknown to most, online privacy policies increasingly purport to govern what can be done with Web site visitors' personal information. Are they in fact binding contracts?

PHOTOILLUSTRATION BY ANDREW CLEMONS

Whether an online visitor discloses personal information during 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 Web site operators can limit their liability for treatment of personal information by disclosing that they might in fact do exactly that. The current legal framework governing privacy policies gives great importance to the concepts of notice and truthful disclosure—i.e., is the Web site 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 Web site 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 Web site company's own interest in attracting and maintaining customers.

Privacy Policies and the Online Trade in Personal Information

A. Online provision of personal information

From the simple act of providing an e-mail address for the purpose of receiving an e-mail newsletter, to 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 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 Web sites afford 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 more than two million active-duty military personnel, *see* Hope Yen, *Data on 2.2M Active Troops Stolen from VA*, Boston Globe Online, June 6, 2006, www.boston.com/news/nation/washington/articles/2006/06/06/veterans_groups_sues_over_data_theft; AOL's disclosure of search data entered by more than 650,000 subscribers, *see* Saul Hansell, *AOL Removes Search Data on Vast Group of Web Users*, N.Y. Times, Aug. 8, 2006, at C4; and the security breach at LexisNexis resulting in improper access to personal information belonging to about 310,000 people, *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. 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.

Lawyers and the public alike should be aware of 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 pernicious, but thoroughly irritating and often expensive, increase in spam.

Concern over online personal privacy has grown considerably over the last 10 years. However, the legislative solution—online privacy policies—may actually decrease protection of consumer information by encouraging Web sites 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 Web sites to appeal to consumers by emphasizing the care with which they treat consumer information. Today, it is rare to visit a Web site that does not have a privacy policy.

Typical privacy policies are accessed via hyperlinks at the bottom of the screen on a Web site's home page. *See, e.g.*, AOL.com Network Privacy Policy, http://about.aol.com/aolnetwork/aol_pp. 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. In a typical provision, Web site users are told that the personal information collected about them may be shared with the Web site's "affiliated providers," with third parties if "necessary to fulfill a transaction" or based on the user's consent. *Id.*

Privacy policies are often incorporated by reference in the Web site's terms of use, which may include a disclaimer of warranties, limitation of liability and a forum selection clause, choice of law provision and/or arbitration clause. While the legislation that requires privacy policies focuses on disclosure of Web site practices to increase consumer awareness, most Web sites in fact present these policies as binding upon visitors, using the language of contract and assent. A typical privacy policy states: "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. … If you do not agree, do not use aol.com." AOL.com, Terms of Use, http://about.aol.com/aolnetwork/aolcom_terms. Many Web sites reserve the right to change their terms of use at any time and advise their users that they are "responsible for checking these terms periodically for changes." *Id.* Users are deemed to have accepted the new terms by continuing to use the Web site after changes are posted to the terms of use.

The end-result of ubiquitous privacy policies that disclose how they use personal information and present themselves as binding upon consumers should be an increase in the actual privacy of consumers' personal information. However, the result of the disclosure approach that has developed seems instead to be the exact opposite: apparent rather than real privacy. 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 percent 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. 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). More recently, 57 percent believed that the mere presence of a privacy policy meant that the Web site could not share consumers' personal information with other Web sites or companies. *Id.* at 4. In fact, a survey in 2000 found that 83 percent of Web site privacy policies allow the site to share personal information with third parties. Anthony D. Miyazaki & Ana Fernandez, *Internet Privacy and Security: An Examination of Online Retailer Disclosures*, 19 J. Pub. Pol'y & Marketing 54 (2000). 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.

If privacy policies are more likely then to contain unfavorable rather than favorable terms, can a

Web site visitor challenge the policy's enforceability?

Privacy Policies and the Law

As applied to most commercial Web sites, 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. No law prevents a Web site operator from sharing or selling personal information it has lawfully been given, although a Web site can be held liable for failing to notify its customers of its practice of selling or sharing such information. As long as they comply with the disclosure requirement, Web sites 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.

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," Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681-1681x (West 1998 & Supp. 2006); protects "customer proprietary network information" from disclosure by telecommunications carriers, 47 U.S.C.A. § 222 (West 2001 & Supp. 2006); regulates how federal governmental agencies gather and handle personal data, Privacy Act of 1974, 5 U.S.C.A. § 552a (West 1996 & Supp. 2006); and requires financial services companies to implement measures to protect the security and confidentiality of their customers' personal information. Gramm-Leach-Bliley Act, 15 U.S.C.A. §§ 6801-6809 (West Supp. 2006).

Federal legislation also specifically aims at dissemination of information held in an electronic format. The "CAN-SPAM Act" prohibits the sending of "unsolicited" e-mail and of misleading header information. 15 U.S.C.A. §§ 7701-7713 (West Supp. 2006). The Computer Fraud and Abuse Act prohibits unauthorized access to a "protected" computer by hackers. 18 U.S.C.A. § 1030(a)(2)(C) (West 2000 & Supp. 2006). Title I of the Electronic Communications Privacy Act (ECPA) prohibits the interception of electronic communications. *Id.* §§ 2710-2712. And Title II of the ECPA (also known as the "Stored Communications Act") prevents improper access to "stored" electronic communications, but does not speak to use of that information. Importantly, there are statutory exceptions under many of the federal statutes for communications where one of the parties has given prior consent to the interception—consent that could come from the Web site's privacy policy.

In addition, the Federal Trade Commission (FTC) interprets Section 5 of the FTC Act—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, or to Web sites' misuse of personal information in the absence of a posted privacy policy pursuant to the "unfair" rather than "deceptive" prong of the statute. 15 U.S.C.A.§ 45(a)(1)-(2) (West 1997). 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.

B. State law

State law too mandates online privacy policies without governing the substance of those policies. Some 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" and requires the entity to limit collection of personal information to that necessary for a "legitimate public purpose." S.C. CODE ANN. § 30-2-40 (West Supp. 2005). And like federal law, state law regulates deceptive or false statements in privacy policies. *See, e.g.*, 18 PA. CONS. STAT. ANN. § 4107 (West Supp. 2006). In addition, an increasing number of states are passing legislation requiring businesses to inform residents if their unencrypted personal information has been compromised. *See, e.g.*, GA. CODE ANN. § 10-1-910 (West Supp. 2006); N.C. GEN. STAT. § 75-65 (2005). Similarly, a number of general application statutes and common law claims have been interpreted to prevent Web sites 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. *See Hill v. MCI Worldcom Communications, Inc.*, 141 F. Supp. 2d 1205, 1209 (S.D. Iowa 2001).

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 Web site companies who violated the terms of their own privacy policies. *See Fed. Trade Comm'n v. ToySmart.com, LLC*, No. Civ.A. 00-CV11341RGS, 2000 WL 1523287 (D. Mass. Aug. 21, 2000). Other enforcement actions have been brought by the FTC for failure to provide adequate security of online personal information in violation of Web sites' own representations that the information would be treated in a secure and safe manner. *See United States v. ChoicePoint Inc.*, No. 1:06-CV-0198 (N.D. Ga. Jan. 30, 2006). 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. *See New York v. Gratis Internet, Inc.*, No. 401210/06, 2006 WL 777061 (N.Y. Sup. Ct. March 22, 2006).

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

D. Private enforcement

Private actions have been unsuccessful in curtailing Web sites' use of personal information in the absence of a broken promise. 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. *See, e.g.*, *In re American Airlines, Inc., Privacy Litigation*, 370 F. Supp. 2d 552 (N.D. Tex. 2005). In those cases, the airlines successfully defended against passengers' claims that the disclosure constituted a violation of their privacy policy by arguing that the policies were not binding. In at least one private enforcement action, a Web site's privacy policy provided some insulation against identity theft claims *because* the policy did not "guarantee" against identity theft.

In one recent case, a man who purchased flowers for his girlfriend via telephone and was directed to the flower company's online privacy policy sued the flower company for violating that policy when it divulged information about the purchase to the man's wife. *Greer v. 1-800-Flowers.com, Inc.*, 2007 WL 3102178 (S.D. Tex. Oct. 3, 2007). The court dismissed the case on the basis of the forum selection clause contained in the flower company Web site's terms of use, which were incorporated by reference in the privacy policy. *Id.* at *2.

The only other significant 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 Web site companies from liability for certain use of personal information because the substantive legislation excepts "authorized" use of the information. *See In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 19-20 (1st Cir. 2003); *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001). 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 Web site 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.

Challenging Enforcement

The most obvious challenge to the enforceability of an online privacy policy as a binding contract is that the Web site visitor failed to assent to the agreement. A contract is only enforceable if both parties have manifested their assent to its terms. E. Allen Farnsworth, Contracts § 3.1 (4th ed. 2004).

An analogy can be made to the online license agreement, about which there is a large body of case law discussing online contract formation. Those cases have found that users are bound to online licenses to which they have "clicked" acceptance or where they have actual notice of the terms. 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. *See Motise v. America Online, Inc.*, 346 F. Supp. 2d 563 (S.D.N.Y. 2004).

Privacy policies are often presented in terms of "browsewrap." Users are deemed to have agreed to them simply by being on the Web site 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, preventing the formation of a binding contract and preventing the Web site from enforcing any of its terms against the consumer. Purported amendments that apply automatically without requiring assent are similarly open to challenge.

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, and its emergence can be linked to the growing use of typical standard form contracts with boilerplate provisions. *See* Charles L. Knapp, Nathan M. Crystal & Harry G. Prince, Problems in Contract Law 667-669 (Aspen Law & Business 4th ed. 1999). The doctrine is codified in Uniform Commercial Code § 2-302 and incorporated in the Restatement (Second) of Contracts § 208 and has been used by courts to police unfairness or one-sidedness in a variety of contract terms. Most states require a showing both of procedural and substantive unconscionability in order to refuse enforcement of a contract term.

Some courts find the procedural unconscionability element satisfied simply by a showing that the agreement at issue is one of adhesion—a standard form agreement offered on a take-it or leave-it basis. The online context is uniquely suited to adhesive agreements, as Web site visitors have no real ability to bargain. Online privacy policies are no exception.

The second prong of the unconscionability argument—substantive unconscionability—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. *See Circuit City Stores, Inc. v. Adams*, 279 F.3d 889 (9th Cir. 2002); *Defontes v. Dell Computers Corp.*, No. C.A. PC 03-2636, 2004 WL 253560 (R.I. Super. Jan. 29, 2004).

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

Finally, as discussed in the *1-800-Flowers.com* case, privacy policies often include a forum selection clause or incorporate by reference such a clause in the Web site's general terms of use. A forum selection clause may be held invalid for being

"unreasonable or unjust." *Forrest v. Verizon Commc'ns, Inc.*, 805 A.2d 1007, 1010-11 (D.C. 2002). Arguments that have been successful in challenging forum selection clauses are that the clause was not readily accessible to the online customer or that the designated forum will effectively deny the plaintiff a legal remedy. 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.

Conclusion

Not all Web sites are required to have privacy policies, but most of them do—and for good reason. Existing legislation and case law allows the Web site to insulate itself from any controls on its use of personal information by providing disclosure, as it focuses on whether a Web site has truthfully revealed what it may in fact do with its customers' personal information. The Web sites 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 be on the horizon. Therefore, if a privacy issue does arise that is arguably governed by the Web site's privacy policy, consumers are likely in the future to want to challenge—not enforce—the policy's binding effect. Rather than providing consumers the protection they expect, privacy policies have become one more online contract of adhesion for consumers to avoid.

Allyson W. Haynes is an associate professor of law at the Charleston School of Law.