

111 Penn St. L. Rev. 587

Penn State Law Review
Winter 2007

Article
Allyson W. Haynes¹

Copyright (c) 2007 The Dickinson School of Law of The Pennsylvania State University; Allyson W. Haynes

ONLINE PRIVACY POLICIES: CONTRACTING AWAY CONTROL OVER PERSONAL INFORMATION?

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 “Webco,” a website visitor named “Vi” discloses certain personal information, including her email address. Soon thereafter, Vi begins to receive numerous unsolicited emails from various advertisers seeking her business. Has Webco violated the law by sharing or even selling Vi’s *588 email address? The answer may lie not in state or even federal legislation, but in a contract that Vi unwittingly entered into when she made the online purchase. In addition, Vi may have agreed that if any dispute arises concerning the use of her personal information, she must arbitrate that claim--again based on an agreement of which she was unaware. Online privacy policies increasingly purport to govern what can be done with website visitors’ personal information.¹ Are they in fact binding contracts?

Whether an online visitor discloses personal information in the course of a purchase or simply because the visitor wishes to receive information in the future, that disclosure is likely the subject of an online privacy policy. Increasingly, privacy policies have become the place where website operators can limit their liability for certain treatment of personal information by disclosing that they might in fact do exactly that.² The current legal framework governing privacy policies gives great importance to the concepts of notice and truthful disclosure³--i.e., is the website treating a consumer’s personal information the way the site promised it would when the consumer provided its personal information to the site? In fact, if the website complies with its own promises, there is little else to prevent the site from doing with the information whatever it wants--sharing, selling or otherwise making use of the information--besides the website company’s own interest in attracting and maintaining customers.⁴

The risk to the website, of course, is that a potential customer will choose not to do business with a particular website that fails to treat his or her personal information in a particular manner.⁵ However, most studies show that, while consumers are increasingly concerned about the privacy of their personal information, they are still not likely to read--much less understand--online privacy policies.⁶ This increases the *589 incentive of a website operator to disclose the potential for broad use of personal information, even if such use is not currently contemplated.⁷

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

Part II discusses how privacy policies have evolved in light of the increase in websites’ use of them and the growing attention to the issue of online privacy in general. Part III discusses the legal framework that governs the posting of privacy policies--both procedural requirements for the posting of privacy policies and more substantive controls over the use of personal information disclosed by online customers--which results in the law being notice-based rather than focused on the

substantive use of personal information. Part IV discusses the disconnect between the growing attention to online treatment of personal information, and actual consumer awareness of how websites treat their personal information. The potential for a website to lose customers based on provisions in their privacy policies is low,⁸ and privacy policies are likely to provide less, rather than more, privacy protection as website operators give themselves the option of sharing or selling customer information. In addition, privacy policies are likely to include other terms that are unfavorable to consumers, including arbitration and forum selection clauses.

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

II. Privacy Policies and the Online Trade in Personal Information

A. Online Provision of Personal Information

Personal information¹⁰ is provided by website visitors¹¹ in numerous ways. From the simple act of providing an email address for the purpose of receiving an email newsletter,¹² to the provision of a credit card number and mailing address to facilitate a purchase,¹³ to the most risky ***591** provision of social security numbers and other financial information to a bank in order to apply for a loan,¹⁴ personal information is given freely and often in the ever-growing online American market.¹⁵

There is growing attention to the security that websites afford such personal information¹⁶ in the wake of recent high-profile personal information disasters, such as the theft of personal information from a Veterans Administration employee, putting at risk the identities of over two million active-duty military personnel;¹⁷ AOL’s recent disclosure of search data entered by more than 650,000 subscribers;¹⁸ and the security breach at LexisNexis resulting in improper access to personal information belonging to about 310,000 people.¹⁹ These events have attuned the public to the importance of the security with which personal information is stored, and the resulting risk of identity theft if such information is lost or stolen.²⁰

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

Concern over online personal privacy has grown from 43% of respondents being “very concerned” and 35% being “somewhat concerned” about threats to their personal privacy in 1990,²³ to an overwhelming 88% of 1,500 Internet users being very or somewhat concerned about websites’ collection of personal information in 2003.²⁴ The issue of personal information privacy even promises to be a factor in ***593** the 2008 presidential election.²⁵ However, the legislative solution--online privacy policies--may actually decrease protection of consumer information by encouraging websites to protect themselves instead.

B. Privacy Policy Terms

Online privacy policies have appeared all over the Internet both in response to increases in legislation requiring such disclosure,²⁶ and as a voluntary measure²⁷ by websites to appeal to consumers by emphasizing the care with which they treat consumer information.²⁸ In 1998, only 2% of all websites had some form of privacy notices,²⁹ and in 1999, eighteen of the top 100 shopping sites did not display a privacy policy.³⁰ By 2001, virtually all of the most popular commercial websites had privacy notices,³¹ with the number continuing to increase through 2005.³² Today ***594** 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 *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.⁴⁰ USATODAY.com tells its visitors that it "reserve[s] the right to use and to disclose to third parties all of the information that we collect online about you and other visitors in any way and for any purpose," except that it will not email promotional offers "directly" to the user unless that user has specifically agreed to receive such promotional materials.⁴¹ Other companies reserve the right to provide users' personal information to third parties for various purposes,⁴² to send email marketing to their users,⁴³ and even to sell users' personal information.⁴⁴

2. Dispute Resolution and Other Terms

Online privacy policies include more than just "privacy" terms. *596 AOL's privacy policy is typical in that it is incorporated by reference in the Aol.com Terms of Use.⁴⁵ Those Terms of Use include a disclaimer of warranties,⁴⁶ limitation of liability,⁴⁷ and a designation of the Commonwealth of Virginia as governing the law and location for resolving any claim or dispute the user may have against AOL.⁴⁸ Amazon.com's Privacy Notice states: "If you choose to visit Amazon.com, your visit and any dispute over privacy is subject to this Notice and our Conditions of Use, including limitations on damages, arbitration of disputes, and application of the law of the state of Washington."⁴⁹

3. Binding Nature of the Policy and Amendments Thereto

While the legislation that requires privacy policies focuses on disclosure of website practices in order to increase consumer awareness, most websites in fact present these policies and amendments thereto as binding upon visitors, using the language of contract and assent. AOL's Terms of Use state: "Your ongoing use of AOL.COM signifies your consent to the information practices disclosed in our Privacy Policy."⁵⁰ AOL reserves the right to change the Terms of Use at any time, and advises the user that he is "responsible for checking these terms periodically for changes."⁵¹ Users are deemed to have accepted the new terms by continuing to use AOL.COM after changes are posted to the Terms of Use.⁵² Similarly, Amazon.com's privacy policy tells its users that "[b]y visiting Amazon.com, you are accepting the practices *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, *598 websites are free to state in their privacy policies that they will treat a visitor's personal information virtually any way they wish, arguably immunizing themselves from liability for such treatment.⁵⁸

A. Federal Law

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

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

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

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

In addition, the Federal Trade Commission ("FTC") interprets Section 5 of the FTC Act⁷³--which prohibits unfair or deceptive acts or practices--as applying to a company's misrepresentations or failure to abide by its own privacy policy statements.⁷⁴ The Act does not require a privacy policy, but provides a means of enforcement of a policy's terms if the company does have one. The FTC has also applied Section 5 to websites' misuse of personal information in the absence of a posted privacy policy pursuant to the "unfair" rather than "deceptive" prong of *600 the statute.⁷⁵

In the past, there has been a push by the federal government to regulate the substance of websites' treatment of personal

information in addition to requiring that certain entities disclose that treatment.⁷⁶ But the proposed legislation was not adopted, and the FTC determined instead to follow the existing self-regulation model, it being “the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology.”⁷⁷ The remains of that proposed substantive legislation are now in the form of “best practices guidelines” or “fair information practices” that encourage disclosure and recommend other privacy practices like security measures and consumer options.⁷⁸

Other aspects of the so-called self-governance model of U.S. privacy policy include privacy seals of approval,⁷⁹ voluntary pledges by *601 websites not to use advertisers unless they have strong privacy policies,⁸⁰ and the development of a “Safe Harbor” agreement with the European Union, whereby U.S. companies wanting to use personal information about EU citizens in the U.S. must recognize more stringent EU prohibitions against using such data.⁸¹

B. State Law

State law too mandates online privacy policies⁸² without governing *602 the substance of those policies.⁸³ And like federal law, state law regulates deceptive or false statements in privacy policies.⁸⁴ In addition, an increasing number of states are passing legislation requiring businesses to inform residents if their unencrypted personal information has been compromised.⁸⁵ Similarly, a number of general application statutes and common law claims have been interpreted to prevent websites from defrauding consumers or violating their privacy statements, but few provide claims for mistreatment of personal information in the absence of some deception or unkept promise.⁸⁶

*603 C. Government Enforcement

Consistent with the focus on disclosure rather than substance, most enforcement with respect to the treatment of personal information has been in the form of FTC enforcement actions brought against website companies who violated the terms of their own privacy policies.⁸⁷ As of August 2006, the FTC had brought actions resulting in eighteen consent agreements or stipulated judgments⁸⁸ pursuant to the Unfair Trade Practices Statute (Section 5 of the FTC Act),⁸⁹ five actions⁹⁰ under the Fair Credit Reporting Act,⁹¹ and eleven actions⁹² pursuant to the *604 Children’s Online Privacy Protection Act (“COPPA”).⁹³

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

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

State attorneys general have brought enforcement actions under the state statutory equivalents of the federal unfair/deceptive practices act that focus primarily on failure to abide by privacy policy terms. Recently, New York’s Attorney General Elliot Spitzer brought an action against Gratis Internet Inc., alleging that the Internet company sold the personal information of approximately seven million people who used its websites, breaching its privacy promises.⁹⁶ Spitzer called the case “the *605 largest deliberate breach of a privacy policy ever discovered by U.S. law enforcement.”⁹⁷ According to the complaint, from 2000 to 2004, Gratis operated six websites through which consumers could obtain free products.⁹⁸ Privacy policies on those sites stated that Gratis would never sell, lend or loan personal information submitted by users of the sites, and specifically promised not to share email addresses.⁹⁹ Nonetheless, during 2004 and 2005 Gratis allegedly sold personal information it had collected to three other firms.¹⁰⁰

New York’s Attorney General has also brought recent actions against Yahoo!,¹⁰¹ Victoria’s Secret,¹⁰² and Chase Manhattan Bank¹⁰³ based on failure to comply with online privacy promises.¹⁰⁴ Yahoo! promised its customers that submitted to its privacy policy that it would not share telephone numbers, but then announced that its privacy policy was being amended to

allow sharing of such numbers.¹⁰⁵ After the state investigation, Yahoo! agreed not to share the numbers or misuse them.¹⁰⁶

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

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

D. Private Enforcement

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

In *In re American Airlines, Inc., Privacy Litigation*,¹¹¹ plaintiffs alleged that American Airlines, Inc. ("American") violated its website's privacy policy when American disclosed passenger information to the Transportation Security Administration ("TSA"). The court dismissed the passengers' breach of contract claim based on American's violation of its promise not to disclose that information because the passengers ***607** failed to allege damages.¹¹² The court also dismissed claims based on Section 2701 of the Wiretap Act because American authorized the third party data collector, Airline Automation, Inc., to disclose the passenger information to the TSA.¹¹³ Furthermore, the court dismissed the ECPA Section 2702 claim because of the statutory exception for disclosure with "the lawful consent of . . . an . . . intended recipient of such communication" (i.e., Airline Automation).¹¹⁴ The disclosure admittedly violated American's privacy policy, but a breach of contract is not "unlawful" in a criminal sense, which is required by the ECPA.¹¹⁵

In *In re Northwest Airlines Privacy Litigation*,¹¹⁶ the court denied recovery to classes of plaintiffs/passengers who alleged that, post 9/11, Northwest Airlines ("Northwest") had breached its privacy policy by providing the National Aeronautics and Space Administration with passenger names, flight numbers, credit card information, hotel and car rental reservations and traveling companions' names.¹¹⁷ The court dismissed the plaintiffs' breach of contract claim, finding that the admittedly-unread privacy policy was a general statement of company policy rather than a contract.¹¹⁸ The court also found that the plaintiffs failed to allege any contract damages.¹¹⁹ In addition, the court dismissed the plaintiffs' claims under the ECPA, finding no improper access to electronic communication service provider information under section 2701, and that Northwest was not an electronic communication service provider under section 2702.¹²⁰

Similarly, in *In re Jetblue Airways Corp. Privacy Litigation*,¹²¹ plaintiff passengers brought a class action for violation of their privacy rights arising out of JetBlue's transfer of passenger personal information to Defendant Torch Concepts, Inc. for use in a federally-funded study on military base security.¹²² The court found claims under New York's ***608** General Business Law and other state consumer protection statutes to be preempted by the ADA.¹²³ The plaintiffs' breach of contract claims based on JetBlue's privacy policy were dismissed because of a failure to allege actual damages;¹²⁴ failure to allege they read the policy was not, however, a ground for dismissal.¹²⁵ Plaintiffs' ECPA section 2702 claim was dismissed because JetBlue is not an electronic communications service provider.¹²⁶

In at least one private enforcement action, a website's privacy policy provided some insulation against identity theft claims because the policy did not "guarantee" against identity theft.¹²⁷ In *Kuhn v. Capital One Financial Corp.*, online customers

brought a putative class action alleging that Capital One failed to respond adequately to a security breach of a retail website server, resulting in loss of customer information.¹²⁸ Plaintiffs' claims included breach of contract based on the online privacy policy.¹²⁹ The court found no misrepresentations in the bank's privacy policy, which included "no guarantee against illicit use" of customer information,¹³⁰ and instead the policy "openly acknowledge[d] the possibility of identity theft and ma[de] no guarantees against its occurrence."¹³¹

The only other private actions concerning privacy policies to date involve the use of third party data collectors, and in those cases the privacy policies potentially exempt the website companies from liability for certain use of personal information because the substantive legislation excepts "authorized" use of the information.¹³² In *609 Crowley v. Cybersource Corp.,¹³³ a customer of Amazon's retail website brought a purported class action against Amazon.com and its third-party verification company, Cybersource Corp., alleging that Cybersource stored customer information in violation of the Wiretap Act and the ECPA.¹³⁴ The plaintiff also brought a claim for breach of contract against Amazon. The court dismissed the Wiretap Act claim, finding that Amazon did not "intercept" an electronic communication from its customer by simply receiving an email from the customer,¹³⁵ and dismissed the ECPA claim because Amazon is not an electronic communication provider under that statute,¹³⁶ and its access to plaintiff's communications was not "unauthorized."¹³⁷

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

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

***610 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 *611 of adults who use the Internet at home, that "years into attempts by governments and advocacy groups to educate people about Internet privacy, the system is more broken than ever."¹⁴⁵ And Chris Hoofnagle reports that "[w]e now have ten years of experience with privacy self-regulation online, and the evidence points to a sustained failure of business to provide reasonable privacy protections."¹⁴⁶

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

The solutions proposed by privacy advocates range from substantive legislation to conform privacy practices to the FTC's Fair Information Practices;¹⁵¹ to "patience" while "market influences such as advertising, *612 personal experience, privacy signals (such as privacy trust marks), and technological developments¹⁵² make privacy terms more salient;"¹⁵³ to encouraging more government enforcement.¹⁵⁴

In the meantime, there is a distinct possibility that as website operators grow savvier with respect to the law, they will respond to the lack of substantive privacy protection (and lack of consumer awareness) by including in privacy policies terms that are not favorable to consumers.¹⁵⁵ Thus, operators will make the cost-benefit calculation that allowing themselves the option of sharing such information in their privacy policies will outweigh any risk that such a provision will prevent consumers from sharing their information in the first place.¹⁵⁶ At the *613 least, such policies will continue to include other non-consumer-friendly terms like arbitration or forum selection clauses.¹⁵⁷

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

V. Challenging Enforcement

A. Lack of Assent

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

An analogy can be made to the online license agreement, about which there is a large body of case law discussing online contract formation.¹⁶¹ Those cases have found that users are bound to online *614 licenses to which they have "clicked" acceptance¹⁶² or where they have actual notice of the terms.¹⁶³ One colorful description of "clickwrap" comes from the District of Massachusetts:

Has this happened to you? You plunk down a pretty penny for the latest and greatest software, speed back to your computer, tear open the box, shove the CD-ROM into the computer, click on "install" and, after scrolling past a license agreement which would take at least fifteen minutes to read, find yourself staring at the following dialog box: "I agree." Do you click on the box? You probably do not agree in your heart of hearts, but you click anyway, not about to let some pesky legalese delay the moment for which you've been waiting. Is that "clickwrap" license agreement enforceable? Yes, at least in the case described below.¹⁶⁴ Users are not bound to license agreements that are only visible to the user by "browsing"--scrolling down the screen or to a different screen--and where the user is not required to view the license in order to complete the transaction.¹⁶⁵

...

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 *619 standard form contracts with boilerplate provisions.¹⁹⁷ The doctrine is codified in the Uniform Commercial Code¹⁹⁸ 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

...

VI. Conclusion

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

In addition to allowing the sites the freedom to do what they wish with personal information, those policies often include other terms that are unfavorable to consumers. While a change in the law to provide substantive privacy protections is the best solution, it does not appear to *624 be on the horizon. Therefore, if a privacy issue does arise that is arguably governed by the website's privacy policy, consumers are likely in the future to want to challenge--not enforce--the policy's binding effect. Their best arguments for doing so are (1) a lack of assent, as many online privacy policies still employ browsewrap acceptance features; and (2) unconscionability of terms like arbitration clauses or unreasonability of forum selection clauses. Rather than providing consumers the protection they expect, privacy policies have become one more online contract of adhesion for consumers to avoid.

Footnotes

- ^{a1} Assistant Professor of Law, Charleston School of Law. J.D., magna cum laude, University of South Carolina School of Law; B.A., Duke University.
- ² See infra Part IV; Anthony D. Miyazaki & Ana Fernandez, Internet Privacy and Security: An Examination of Online Retailer Disclosures, 19 J. Pub. Pol'y & Marketing 54, 58 (2000) (finding only 17% of commercial websites surveyed disclosed that they would not share personal information with third parties).
- ⁵ Customers are finding out about these breaches more often now that legislation requires notification. See infra note 86. As a result, consumers may boycott websites that disclose personal information. Katherine J. Strandburg, [Privacy, Rationality, and Temptation: A Theory of Willpower Norms](#), 57 Rutgers L. Rev. 1235, 1286 (2005).
- ⁶ "In a study of adult Internet users who were asked to evaluate the credibility of Web sites, less than one percent of respondents even noticed privacy policies." James P. Nehf, [Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy](#), 2005 U. Ill. J.L. Tech. & Pol'y 1, 11 (2005) (citing B.J. Fogg, et al., How Do People Evaluate a Web Site's Credibility?: Results from a Large Study 1, 86 (2002), <http://www.consumerwebwatch.org/pdfs/stanfordPTL.pdf>). Researchers have found that "online information privacy is important to consumers and that consumers desire more control over access to their personal information and subsequent use of the information after it is obtained," Nehf at 5, which would suggest that consumers would take steps to protect their privacy by frequenting websites that have favorable policies and avoiding those that do not. However, "research on bounded rationality and consumer decision making suggests that in most circumstances consumers, acting rationally, do not factor privacy policies into

their decision processes, even when they consider privacy important, because privacy concerns are seldom salient.” Id. See also M.J. Culnan & G.R. Milne, *The Culnan-Milne Survey of Consumers and Online Privacy Notices: Summary of Responses 1, 2* (2001), <http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf> (consumers still do not seem to read online privacy policies); Humphrey Taylor, *Most People Are “Privacy Pragmatists” Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits*, *The Harris Poll No. 17*, March 19, 2003, http://www.harrisinteractive.com/harris_poll/index.asp?PID=365.

- ¹⁰ The term “personal information” is used here as it is defined under federal law: [I]ndividually identifiable information about an individual collected online, including--(A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.
- Children’s Online Privacy Protection Act of 1998, [15 U.S.C.A. § 6501\(8\)](#) (West Supp. 2006).
- In the financial realm, federal law defines nonpublic personal information as “personally identifiable financial information--(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.” Gramm-Leach-Bliley Act of 1999, [15 U.S.C.A. § 6809\(4\)](#) (West Supp. 2006); see also [18 U.S.C.A. § 2725\(3\)](#) (West 2000) (“[P]ersonal information’ means information that identifies an individual, including an individual’s photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver’s status.”).
- ¹¹ The website visitor who provides his or her personal information to a website is variously referred to in this article as a “visitor,” “user,” or “consumer.”
- ¹² For example, L.L.Bean’s website invites visitors to “Sign up for our Email Newsletter and learn about our latest products and sale events. It’s easy to subscribe--just enter your email address below.” L.L.Bean: Email Newsletter, <http://www.llbean.com> (follow “Email Newsletter” hyperlink) (last visited Jan. 31, 2007).
- ¹³ Like many retail sites, Target.com allows a user to create an account including the user’s mailing address and credit card number so that the user can conveniently make a purchase with only one click of her mouse. See Target.com: My Account, <http://www.target.com> (follow “my account” hyperlink) (last visited Jan. 31, 2007).
- ¹⁴ See CitiFinancial: What You Can Expect, <https://secure.citifinancial.com/common/whatyoucanexpect.php> (last visited Jan. 31, 2007).
- ¹⁵ In 2005, total e-commerce sales in the United States were estimated at \$86.3 billion, an increase of 24.6% from 2004. These online sales accounted for 2.3% of total sales in the country, up from 2.0% of total sales in 2004. U.S. Census Bureau News, *Quarterly Retail E-commerce Sales, 4th Quarter 2005* (Feb. 17, 2006), <http://www.census.gov/mrts/www/data/html/05Q4.html>.
- ¹⁶ There has also been increased attention to the threat of online sexual predators, particularly those who target children. See Chelsea Kellner, *Web Site Builds Web of Friends*, *Pittsburgh Tribune-Review*, Feb. 7, 2006, at E4 (discussing how websites like Myspace.com and Facebook.com pose challenges to law enforcement because they allow predators to identify young people by the personal information they provide); SAFE ONLINE: History of Local Stories, *Eyewitness News*, <http://www.eyewitnessnewstv.com> (hover over “Special Reports” hyperlink; then hover over “Know More Links” hyperlink; then follow “Archived Story Links” hyperlink; then follow “SAFE ONLINE: History of Local Stories” hyperlink) (last visited Jan. 31, 2006) (discussing recent stories about friend-networking websites like Myspace, and adults pursuing children online).

- ¹⁷ See Hope Yen, Data on 2.2M Active Troops Stolen from VA, ABC News, June 6, 2006, <http://www.abcnews.go.com> (search for “Data on 2.2M Active Troops Stolen from VA”) (noting that records on file for almost all active-duty personnel—including as many as 1.1 million active-duty personnel from all the armed forces, along with 430,000 members of the National Guard, and 645,000 members of the Reserves—had been stolen in what has become “one of the nation’s largest security breaches”).
- ¹⁸ See Saul Hansell, AOL Removes Search Data on Vast Group of Web Users, N.Y. Times, Aug. 8, 2006, at C4 (describing AOL’s release of Internet search terms from more than 650,000 subscribers over a three-month period and its acknowledgement that the search queries themselves may contain personally identifiable information).
- ¹⁹ See David Colker, LexisNexis Breach Is Larger: The Company Reveals that Personal Data Files on as Many as 310,000 People Were Accessed, L.A. Times, Apr. 13, 2005, at C1.
- ²⁰ See generally Privacy Rights Clearinghouse, A Chronology of Data Breaches, <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (last visited Jan. 31, 2007) (maintaining a running total of records compromised by security breaches). To date, over 100 million records have been put at risk as a result of security breaches at companies holding sensitive consumer information. *Id.*; see also Data Theft Due to Criminal Intent is a Reality Now, Fin. Express, July 25, 2005, available at 2005 WLNR 11611049 (discussing security breach of cardholder information held by Cardsystems); Another Week, Another Identity Theft Scandal: Recent Data Security Breaches Underscore Need for Stronger Identity Theft Protections, <http://www.consumersunion.org/creditmatters/creditmattersupdates/002244.html> (describing recent security breaches of information owned by LexisNexis, ChoicePoint, Bank of America, and Ameritrade among others and detailing protection laws that Consumer Union is attempting to enact) (last visited Jan. 31, 2007).
- ²¹ An example is the sale by ChoicePoint, one of the country’s largest data brokers, of personal data of approximately 162,000 individuals to identity thieves. See Daniel J. Solove & Chris Jay Hoofnagle, [A Model Regime of Privacy Protection](#), 2006 U. Ill. L. Rev. 357, 358 (2006) (describing the ChoicePoint debacle); Michael Hiltzik, Big Data Broker Eyes DMV Records, L.A. Times, Dec. 1, 2005, at C1 (noting that ChoicePoint not only sold personal information of 162,000 people to L.A. identity thieves but also has been accused of such unauthorized sales before); Joseph Menn, Did the ChoicePoint End Run Backfire?, L.A. Times, Mar. 13, 2005, at C1 (describing the ChoicePoint incident and predicting tighter regulation on collection of personal data); Bob Sullivan, Database Giant Gives Access to Fake Firms: ChoicePoint Warns More than 30,000 They May be at Risk, MSNBC, Feb. 14, 2005, <http://www.msnbc.msn.com/id/6969799> (detailing ChoicePoint incident and the risks consumers face as a result of security breach).
- ²² According to Jupiter Research, “American consumers will receive an estimated 645 billion commercial email messages in the year 2007.” Linda A. Goldstein, Online Advertising: Rules of the Net, 822 PLI/Pat 291, 325 (2005). Congress has recognized that “[t]he convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail,” and that such mail “may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail” as well as impose “significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and receive such mail.” Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 2(a), 117 Stat. 2699, 2699 (2003).
- ²³ Public Opinion on Privacy, Elec. Privacy Info. Ctr., <http://www.epic.org/privacy/survey/> (last visited Jan. 31, 2007) (citing Privacy in America and Consumers in the Information Age, The Harris Poll, January 1990 (study number 892049)).
- ²⁴ Anne Kandra & Andrew Brandt, The Great American Privacy Makeover, 21 PC World, Oct. 8, 2003, at 145-146, available at <http://www.pcworld.com/article/id,112468-page,1-c,privacy/article.html>.
- ²⁵ Cf. Clinton Touts Privacy Bill of Rights, Newsday, June 17, 2006, at A16 (“[Senator] Clinton wants a ‘privacy czar’ within the White House to guard against recent problems like the recent theft of personal data from Department of Veterans Affairs. She also

wants legislation to let consumers know what information companies are keeping about them and how it is used, and... with penalties for companies who are not careful with personal data.”).

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

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

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

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

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.*

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

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

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

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

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

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

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

⁶⁶ Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (“CAN-SPAM Act”), [15 U.S.C.A. §§ 7701-7713 \(West Supp. 2006\)](#). Of course, if a website company’s privacy policy provides that a visitor agrees to receive email communications, the company does not violate the Act by sending email.

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

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

⁶⁹  [18 U.S.C.A. § 2511\(2\)\(d\) \(West 2006\)](#).

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

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

⁷² *Id.* § 2702(b)(3).

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

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

⁷⁵ See [In re BJ’s Wholesale Club, Inc., 140 F.T.C. 465, 2005 FTC LEXIS 134 \(2005\)](#).

⁷⁶ The FTC issued a report to Congress examining the issue of online privacy in 2000, which stated that “ongoing consumer concerns regarding privacy online and limited success of self regulatory efforts to date make it time for government to act to protect consumers’ privacy on the Internet.” See Fed. Trade Comm’n, *Privacy Online: Fair Information Practices in the Electronic Marketplace 28-29* (2000), available at [http:// www.ftc.gov/reports/privacy2000/privacy2000.pdf](http://www.ftc.gov/reports/privacy2000/privacy2000.pdf). The FTC voted three to two to recommend that Congress enact legislation to ensure adequate protection of consumer privacy by requiring all consumer-oriented websites that collect personal identifying information to establish privacy policies in accordance with the four “Fair Information Practice Principles” (“FIPP”). *Id.*

⁷⁷ *Self-Regulation & Privacy Online: Statement Before the House Commerce Subcomm. on Telecomm., Trade, and Consumer Prot. of the H. Comm. on Commerce, 106th Cong. (1999)*, available at [http:// www.ftc.gov/os/1999/07/pt071399.htm](http://www.ftc.gov/os/1999/07/pt071399.htm) (statement of the Federal Trade Commission). By 2001, FTC Chairman Timothy J. Muris noted that a majority of the Commission was not in favor of online privacy legislation at that time. *Challenges Facing the Fed. Trade Comm’n: Hearing Before the Subcomm. on Commerce,*

Trade, and Consumer Protection of the H. Comm. on Energy and Commerce, 107th Cong. (2001) (statement of Timothy J. Muris, Chairman, Federal Trade Commission), 2001 WL 1383075; see also Nehf, *supra* note 6, at 3 (describing how self-regulation resulted from the FTC's threat to pass privacy legislation if Internet firms did not adopt fair information practices in due course: "Because the market for consumer purchasing, demographic, and Web-surfing information was in full swing with a seemingly unlimited future, firms with strong online presences overwhelmingly preferred self-regulation to mandatory privacy standards that might hinder further growth. It was therefore in the interest of the major online firms to encourage smaller firms to adopt privacy practices that satisfied the FTC.").

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

⁷⁹ Websites may earn a privacy "seal of approval" from an entity such as TRUSTe (www.truste.org), the Council of Better Business Bureaus (www.bbbonline.org), the American Institute of Certified Public Accountants, WebTrust (www.cpawebtrust.org), or the Entertainment Software Rating Board (www.esrb.org/privacy), by conforming to certain guidelines. See Business Roundtable Report, *supra* note 27, at 15 ("The primary self-regulatory enforcement initiatives are the online seal programs which require 'licensees' to implement fair information practices and to submit to various types of compliance monitoring to display a privacy seal on their Web sites.... According to the FTC, the online seal programs have not yet established a significant presence on the Web.").

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

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

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

Other state laws require certain entities like governmental agencies to post privacy policies. For instance, South Carolina's Family Privacy Protection Act requires the posting of privacy policies by any state entity "which hosts, supports, or provides a link to page or site accessible through the world wide web." *S.C. Code Ann. § 30-2-40* (West Supp. 2005). See also *Ariz. Rev. Stat. Ann. §§ 41-4151-52* (2004 & Supp. 2006); *Ark. Code Ann. § 25-1-114* (Supp. 2005); *Cal. Gov't Code § 11019.9* (West 2005); *Colo. Rev. Stat. §§ 24-72-501-02* (2006); *Del. Code Ann. tit. 29, §§ 9017C-9018C* (2006); 5 *Ill. Comp. Stat. 177/10(b)(2)* (West 2005); *Iowa Code Ann. § 22.11* (West 2001); *Me. Rev. Stat. Ann. tit. 1, §§ 541-42* (Supp. 2006); *Md. Code Ann., State Gov't § 10-624(c)(4)* (LexisNexis 2004); *Mich. Comp. Laws Serv. § 205.827* (LexisNexis Supp. 2006); *Minn. Stat. Ann. § 13.15* (West 2005); *Mont. Code Ann. §§ 2-17-550-53* (2005); *N.Y. State Tech. Law §§ 201-07* (2006); *Tex. Gov't Code Ann. § 2054.126* (Vernon Supp. 2006); *Va. Code Ann. §§ 2.2-3800-03* (2005).

⁸³ California's law requires disclosure of privacy practices and access to personal information, but does not regulate how the website

might treat that information if it in fact discloses that treatment. Online Privacy Protection Act of 2003, [Cal. Bus. & Prof. Code § 22575](#) (West Supp. 2007). The session law implementing the Act noted that it was “the intent of the Legislature to require each operator of a commercial Web site or online service to provide individual consumers residing in California who use or visit the commercial Web site or online service with notice of its privacy policies, thus improving the knowledge these individuals have as to whether personally identifiable information obtained by the commercial Web site through the Internet may be disclosed, sold, or shared.” 2003 Cal. Stat. 829 § 2(b). Other state laws require security provisions but do not otherwise govern use of personal information. For example, Michigan requires any person who obtains one or more social security numbers in the ordinary course of business to create a privacy policy that provides security and prevents access. Mich. Comp. Laws Serv. § 445.84 (LexisNexis 2006).

⁸⁴ New York applies its statute, [N.Y. Gen. Bus. Law § 349](#) (McKinney 2004), which prohibits deceptive practices and false advertising, to a website’s privacy promises. See [Fed. Trade Comm’n v. Crescent Publ’g Group, Inc.](#), 129 F. Supp. 2d 311, 319 (S.D.N.Y. 2001). Pennsylvania makes it illegal for a collector of personal information to knowingly make a false or misleading statement in a published privacy policy about how it will use that information. [18 Pa. Cons. Stat. Ann. § 4107](#) (West Supp. 2006).

⁸⁵ See, e.g., [Ariz. Rev. Stat. Ann. § 44-7501](#) (West Supp. 2006); [Ark. Code Ann. §§ 4-110-105](#) (Supp. 2005); [Cal. Civ. Code §§ 1798.29](#) (West Supp. 2006); [Colo. Rev. Stat. § 6-1-716](#) (2006); [Conn. Gen. Stat. Ann. §§ 36a-701](#); 36a-701a; 36a-701b (West Supp. 2006); [Del. Code Ann. tit. 6, §§ 12B-101-04](#) (2005); [Fla. Stat. § 817.568](#) (West 2006); [Ga. Code Ann. § 10-1-910](#) (West Supp. 2006); [Haw. Rev. Stat. § 487N-2](#) (2006); [815 Ill. Comp. Stat. 530/12](#) (2006); [Ind. Code Ann. § 4-1-11-5](#) (LexisNexis Supp. 2006); [La. Rev. Stat. Ann. § 51:3074](#) (Supp. 2007); [Me. Rev. Stat. Ann. tit. 10, § 1348](#) (Supp. 2006); [Minn. Stat. Ann. § 325E.61](#) (West Supp. 2006); [Mont. Code Ann. § 31-3-115](#) (2005); [Nev. Rev. Stat. Ann. § 603A.220](#) (LexisNexis Supp. 2006); [N.H. Rev. Stat. Ann. § 359-C:20](#) (LexisNexis Supp. 2006); [N.J. Stat. Ann. § 56:8-163](#) (West Supp. 2006); [N.Y. Gen. Bus. Law § 899-aa](#) (McKinney Supp. 2007); [N.C. Gen. Stat. § 75-65](#) (2005); [N.D. Cent. Code § 51-30-02](#) (Supp. 2005); [Ohio Rev. Code Ann. §§ 1347.12](#); 1349.19 (West Supp. 2006); [73 Pa. Stat. Ann. § 2303](#) (West Supp. 2006); [R.I. Gen. Laws § 11-49.2-3](#) (Supp. 2006); [Tenn. Code Ann. § 47-18-2107](#) (Supp. 2006); [Tex. Bus. & Com. Code Ann. § 48.103](#) (Vernon Supp. 2007); [Wash. Rev. Code § 19.255.010](#) (West Supp. 2006). For a discussion of these laws and a list that is periodically updated, see State PIRG Summary of State Security Freeze and Security Breach Notification Laws, The State PIRG Consumer Protection Inside Pages, <http://www.pirg.org/consumer/credit/statelaws.htm> (lasted visited Jan. 31, 2007).

⁸⁶ Some states have general application statutes prohibiting “invasion of privacy” or “intrusion upon seclusion” that may be asserted in a variety of situations where consumers’ information is unexpectedly or unreasonably used, sold or shared. See [Hill v. MCI Worldcom Commc’ns, Inc.](#), 141 F. Supp. 2d 1205, 1209 (S.D. Iowa 2001) (disclosure of phone numbers and addresses of consumer’s friends to a stalker was cognizable as invasion of privacy); [Remsburg v. Docusearch, Inc.](#), 816 A.2d 1001 (N.H. 2003) (finding that Docusearch.com, an investigation service, may be held liable for negligence or invasion of privacy for selling personal information to a client over the Internet, where that client used the information to track and murder New Hampshire resident Amy Boyer); [McGuire v. Shubert](#), 722 A.2d 1087, 1090 (Pa. Super. Ct. 1998) (a customer whose bank account information has been disclosed by the bank to a third party may have a cause of action for invasion of privacy).

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

**Stuart, Allyson 4/12/2019
For Educational Use Only**

ONLINE PRIVACY POLICIES: CONTRACTING AWAY..., 111 Penn St. L. Rev. 587

- ⁸⁸ See, e.g., *United States v. ChoicePoint Inc.*, No. 1:06-CV-0198 (N.D. Ga. Jan. 30, 2006); *Fed. Trade Comm'n v. ToySmart.com, LLC*, No. Civ.A. 00-CV11341RGS, 2000 WL 1523287 (D. Mass. Aug. 21, 2000); *DSW Inc.*, 70 Fed. Reg. at 73,474; *CardSystems Solutions, Inc.* 71 Fed. Reg. 10,686 (Fed. Trade Comm'n March 2, 2006) (analysis of proposed consent order); *In re BJ's Wholesale Club, Inc.*, 2005 FTC LEXIS 134, at *1; *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102, 113, 2005 FTC LEXIS 40 (2005); *In re Vision I Props., LLC*, 139 F.T.C. 296, 302; 2005 FTC LEXIS 66 (2005); *In re Gateway Learning Corp.*, 2004 FTC LEXIS 150, at *10 (2004); *In re MTS, Inc. d/b/a Tower Records/Books/Video*, 2004 FTC LEXIS 88, at *8 (2004); *In re Educ. Research Ctr. of Am., Inc.*, 2003 FTC LEXIS 72, at *10 (2003); *In re Guess?, Inc.*, 2003 FTC LEXIS 123, at *10 (2003); *In re Nat'l Research Ctr. for Coll. & Univ. Admissions, Inc.*, 2003 FTC LEXIS 9, at *10 (2003); *In re Eli Lilly & Co.*, 2002 FTC LEXIS 22, at *9 (2002); *In re Microsoft Corp.* 2002 FTC LEXIS 43, at *11 (2002); *In re GeoCities*, 127 F.T.C. 94, 1999 FTC LEXIS 17, at *11 (1999); *In re Liberty Fin. Cos.*, 1999 FTC LEXIS 46, at *5 (1999).
- ⁸⁹ See 15 U.S.C.A. § 45(a) (West 1997).
- ⁹⁰ See, e.g., *In re Quicken Loans Inc.*, 2002 FTC LEXIS 96, at *6 (2002); *In re First Am. Real Estate Solutions, LLC*, 1998 FTC LEXIS 115, at *5 (1998).
- ⁹¹ See 15 U.S.C.A. § 1681 (West 1998).
- ⁹² See, e.g., *United States v. Hershey Foods Corp.*, Civ. No. 4:03-cv-00350-JEJ (M.D. Pa. Feb. 26, 2003); *United States v. Mrs. Fields Famous Brands*, Civ. No. 2:03cv00205 (D. Utah Feb. 25, 2003); *United States v. Ohio Art Co.*, Civ. No. 3:02CV7203 (N.D. Ohio Apr. 30, 2002); *United States v. Am. Pop Corn Co.*, Civ. No. C02-4008DEO (N.D. Iowa Feb. 28, 2002); *United States v. Lisa Frank, Inc.*, Civ. No. 01-1516-A (E.D. Va. Oct. 3, 2001); *United States v. Looksmart, Ltd.*, Civ. No. 01-606-A (E.D. Va. Apr. 23, 2001); *United States v. Bigmailbox.com, Inc.*, Civ. No. 01-605-A (E.D. Va. Apr. 23, 2001); *United States v. Monarch Servs., Inc.*, Civ. No. AMD 01 CV 1165 (D. Md. Apr. 20, 2001); *In re Bonzi Software, Inc.*, 2004 FTC LEXIS 206, at *10 (2004).
- ⁹³ See Children's Online Privacy Protection Act of 1998,  15 U.S.C.A. § 6501 (West Supp. 2006).
- ⁹⁴ See *United States v. ChoicePoint Inc.*, No. 1:06-CV-0198 (N.D. Ga. Jan. 30, 2006); *In re Petco Animal Supplies, Inc.*, 2005 FTC LEXIS 40, at *1; *In re MTS, Inc. d/b/a Tower Records/Books/Video*, 2004 FTC LEXIS 88, at *8; *In re Guess?, Inc.*, 2003 FTC LEXIS 123, at *10; *In re Eli Lilly & Co.*, 2002 FTC LEXIS 22, at *9; *In re Microsoft Corp.*, 2002 FTC LEXIS 43, at *11.
- ⁹⁵ See *Fed. Trade Comm'n v. ToySmart.com, LLC*, No. Civ.A. 00-CV11341RGS, 2000 WL 1523287 (D. Mass. Aug. 21, 2000) (bankrupt retail toystore offered customer lists for sale in violation of privacy policy); *In re Vision I Props., LLC*, 139 F.T.C. at 302 (retail merchants who use CartManager often had privacy policies saying they would not share personal information, but CartManager rented that information); *In re Gateway Learning Corp.*, 2004 FTC LEXIS 150, at *10 (educational products company rented personal information provided online despite privacy statements to the contrary); *In re Educ. Research Ctr. of Am., Inc.*, 2003 FTC LEXIS 72, at *10 (companies' marketing materials and privacy statements stated that survey information collected offline from school students would only be shared with educational entities, but information was in fact shared with third party marketers for commercial purposes); *In re GeoCities*, 1999 FTC LEXIS 17, at *11 (online privacy statements misrepresented purposes for collecting personal information and that information would not be disclosed to third parties without permission).
- ⁹⁶ See *New York v. Gratis Internet, Inc.* No. 401210/06, 2006 WL 777061 (N.Y. Sup. Ct. Super. Ct. March 22, 2006).
- ⁹⁷ *Web Firm Sold Info of 7 Million People, New York Suit Claims*, 23 No. 22 *Andrews Computer & Internet Litig. Rep.* 11 (Apr. 4, 2006).

¹²⁰ Id. at *2. See also [Dyer v. Northwest Airlines Corps.](#), 334 F. Supp. 2d 1196 (D.N.D. 2004). In *Dyer*, the plaintiff's ECPA section 2702 claim was dismissed because Northwest is not an electronic communications service provider and the breach of contract claim was dismissed because it was based on a privacy policy and the court found it a policy, not a contract. See [id.](#) at 1200. The plaintiffs made no allegation that they logged onto a website or read a privacy policy and made no allegation of damages. Id.

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

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

¹⁴² Nehf, *supra* note 6, at 3-4.
[P]rivacy policies can be seen everywhere today, and they give the impression that Web sites safeguard personal information that they collect. When the policies are read, however, there is often very little privacy protection being promised. Policies might disclose how data is collected and how it will be transferred, sold, or traded, but often the message is that information will be collected in whatever way the Web site can obtain it, and the site reserves the right to share or sell it with impunity. References to information security or safeguards tend to be vague and noncommittal. Thus, despite the proliferation of privacy policies online, consumers' privacy interests may in fact be no better protected today than they were ten years ago.
Id. (footnotes omitted); see also Solove & Hoofnagle, *supra* note 21, at 357 (opining that current U.S. privacy law does not adequately address the activities of the database industry, and suggesting certain changes in legislation, including universal notice of all companies collecting personal information, ensuring meaningful informed consent about the uses and dissemination of PI, the ability of consumers to manage their credit records and ensure the accuracy of their PI, and various security measures); Katherine J. Strandburg, [Privacy, Rationality & Temptation: A Theory of Willpower Norms](#), 57 *Rutgers L. Rev.* 1235, 1286 (2005).
Consumers as a whole might be better off penalizing sites that do not offer a high level of privacy protection by refusing to deal with them, but for each individual consumer it is rational to attempt to free ride on the boycott efforts of others. Consumers are unable to enforce a boycott because they cannot detect and penalize defectors. This analysis suggests that consumers will not be able to sustain a 'norm against tempters' that penalizes such websites.
Id. (footnotes omitted); Richard Warner, [Surveillance & the Self: Privacy, Identity, & Technology](#), 54 *DePaul L. Rev.* 847, 848 (2005) (arguing that "[t]o ensure sufficient power [to control what others can learn about us and what they can do with what they learn], businesses should be required to obtain our consent before they collect certain types of information about us," and that "the 'consent requirement' is insufficient on its own to protect privacy adequately," so additional statutory protection is necessary).

¹⁴³ See Nehf, *supra* note 6, at 3-4.
The FTC lauded the success of its market-driven solution. The FTC placed its faith in market incentives to curb unfair privacy practices, but there may be little incentive for online businesses to adopt and adhere to strong privacy policies. It is the appearance of privacy that seems to matter most.
Id. (footnotes omitted) (emphasis added).

¹⁴⁴ David A. DeMarco, Note, [Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood & Pragmatism, Pop-tarts & Six-packs](#), 84 *Tex. L. Rev.* 1013, 1047 (2006) (stating that Amazon.com's privacy policy "gives only vague notice regarding how it uses information and offers only a very limited extent of control--basically an all-or-nothing choice--over how submitted personal information can be used").

- ¹⁴⁹ Miyazaki & Fernandez, *supra* note 1, at 58 (finding only 17% of websites surveyed disclosed that they would not share personal information with third parties).
- ¹⁵⁰ See DeMarco, *supra* note 145, at 1047 (“[S]ince there are few legal restraints on what the company can do with information once the information is in its hands and since customers are not very demanding with regard to the ways in which their information may be utilized, it makes good business sense to keep the policy as vague as possible.”); Nehf, *supra* note 6, at 43 n.220 (noting that after the passage of federal legislation like the GLBA and HIPAA, “legions of lawyers” have become involved in drafting privacy policies that are lengthier and more difficult to understand than even before); Turow, *supra* note 53, at 9-10 (discussing “world of legalistically phrased privacy policies” that are long, ambiguous, and hard to read).
- ¹⁵¹ In March 2005, the Electronic Privacy Information Center (“EPIC”) issued a study arguing that after “ten years of experience with privacy self-regulation online, and the evidence points to a sustained failure of business to provide reasonable privacy protections.” Hoofnagle, *supra* note 110, at 1. EPIC calls upon the FTC and Congress “to create a floor of standards for protection of personal information based on Fair Information Practices.” *Id.* Daniel Solove and Chris Hoofnagle have proposed a Model Privacy Regime to address problems in United States privacy protection, aiming “to patch up the holes in existing privacy regulation and improve and extend it.” Solove & Hoofnagle, *supra* note 21, at 357. Solove and Hoofnagle suggest sixteen methods in which the Fair Information Practices advocated by the FTC in its self-regulation approach should instead be incorporated into specific legislation. *Id.*
- ¹⁵² Technological solutions include software options like the Platform for Privacy Preferences (“P3P”), which is an industry-promoted software solution to online privacy concerns that allows consumers to choose what information they wish to share with websites and for what purposes. When a site seeks additional information or wants to use the information for other purposes, the user’s browser displays a warning. See Kimberly Rose Goldberg, Note, [Platform for Privacy Preferences \(“P3P”\): Finding Consumer Assent to Electronic Privacy Policies](#), 14 *Fordham Intell. Prop. Media & Ent. L.J.* 255, 256 (2003).
- ¹⁵⁴ The FTC and state attorneys general have used their unfair trade practices statutes to target online companies that violate their privacy policies, or that negligently fail to provide adequate security to consumers’ personal information. These agencies could broaden the scope of that enforcement to include privacy practices whereby a website obtains a consumer’s information for one purpose and later uses it for another, or unreasonably shares or sells such information. The problem here is that websites’ privacy policies are increasingly likely to give them that very ability. The FTC is unlikely to find any practice “unfair” that is specifically allowed by the privacy policy. As Professor Nehf noted, “The FTC will declare a practice unfair only if the injury is not one that consumers can reasonably avoid. The FTC views its role as promoting consumer choice, not second-guessing those choices. It will not change market outcomes when the injury can be avoided by consumers taking reasonable actions themselves.” *Id.* at 46 (citations omitted). However, the FTC has brought actions against firms that “take advantage of poorly informed decision making,” suggesting that consumers may be able to challenge the idea that they could have “reasonably avoided” the privacy injury. *Id.* at 50. As Professor Nehf pointed out, consumers may argue that it would be unreasonable to require that they read a privacy policy, understand its implications, and take protective action. *Id.*
- ¹⁵⁵ Researchers have found that, by using certain techniques in framing and wording of questions, website operators can almost guarantee a “yes” answer. Public Opinion on Privacy, Elec. Privacy Info. Ctr., [http:// www.epic.org/privacy/survey/](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.”).
- ¹⁵⁸ First, the visitor is usually unaware of the policy, much less that any increase in unsolicited email or risk of identity theft is due to the particular website’s sharing of information. Second, as discussed above, without the breach of a privacy policy there is little substantive law to prevent the sale or sharing of personal information. Finally, there are many practical problems with a law suit based on a website’s sharing of personal information, including the requirement that the visitor prove damages. See *infra* notes 188-90 and accompanying text.

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

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

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

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

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

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

¹⁹¹ One additional reason why privacy policies may fail to bind consumers is a result of their tendency to "invite" rather than require the user to view the policy. In [Specht v. Netscape Commc'ns Corp.](#), 150 F. Supp. 2d 585, 596 (S.D.N.Y. 2001) (footnote omitted), the court noted that the individual obtaining Netscape's SmartDownload software is not made aware that he is entering into a contract: Couched in the mild request, "Please review [and agree to the terms of the license agreement before downloading]," this language reads as a mere invitation, not as a condition. The language does not indicate that a user must agree to the license terms before

downloading and using the software. While clearer language appears in the License Agreement itself, the language of the invitation does not require the reading of those terms or provide adequate notice either that a contract is being created or that the terms of the License Agreement will bind the user.

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

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

 [Id.](#) at 556-57.

¹⁹³ See supra Part II.

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

¹⁹⁵ *Id.* Similarly, Yahoo! purported to amend its privacy policy, announcing that telephone numbers submitted with the understanding that they would not be shared would not be shared. Attorney General of the State of New York, Internet Bureau, In re Yahoo! Inc., Assurance of Discontinuance (Sep. 24, 2003), available at <http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/nys/nygyahoo92403aod.pdf>. After New York’s Attorney General investigated, the company agreed not to share the numbers or misuse them. *Id.*

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?”).

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

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).