Minding Your Own Business: Privacy Policies in Principle and in Practice

Scott Killingsworth
Powell, Goldstein, Frazer & Murphy

Follow this and additional works at: https://digitalcommons.law.uga.edu/jipl
Part of the Contracts Commons, and the Intellectual Property Law Commons

Recommended Citation
Available at: https://digitalcommons.law.uga.edu/jipl/vol7/iss1/3

This Article is brought to you for free and open access by Digital Commons @ Georgia Law. It has been accepted for inclusion in Journal of Intellectual Property Law by an authorized editor of Digital Commons @ Georgia Law. Please share how you have benefited from this access. For more information, please contact tstriepe@uga.edu.
MINDING YOUR OWN BUSINESS: PRIVACY POLICIES IN PRINCIPLE AND IN PRACTICE

Scott Killingsworth*

I. INTRODUCTION

For e-commerce websites, having a privacy policy is no longer optional. Federal legislation, FTC enforcement, the European Union Privacy Directive,¹ economic coercion and consumer demand have all recently converged to create a new environment in which implementing a privacy policy is a business necessity for most, and legally advisable for all.

In principle, privacy policies are simple: if your website collects individually-identifying information about visitors or customers, tell them how and why you collect the information, how it is used and to whom it is disclosed, and give them some choice in the matter. But the short history of personal privacy on the web is already replete with examples of how treacherous the execution of this simple formula can be: Internet icons like Yahoo, DoubleClick, America Online and GeoCities, and major corporations like United Airlines, have all stumbled on privacy issues. The hazards are many: first, the emerging legal rules, self-regulation models and web-community norms are all moving targets; second, though consistent in thrust, the legal rules differ in important details; and third, there is a noticeable gap between what is legal and what may be necessary to avoid a public-relations disaster. Applying these fragmented, evolving principles to a web-based business that is itself in constant flux can be like trying to thread a needle while roller skating on a boat in choppy seas.

This article describes how to design a website privacy policy that will be effective both legally and in practice. It addresses specific issues that must be confronted in drafting and implementing a policy, and offers suggestions for

avoiding pitfalls. But we begin with context: the business pressures that make a privacy policy necessary and the legal principles that apply.

II. “YOU HAVE ZERO PRIVACY ANYWAY. GET OVER IT.”

Scott McNealy’s impulsive remark to a roomful of reporters could hardly be more politically incorrect, but it mirrors the perceptions of many on both sides of the privacy fence. On the one hand, some website operators have avidly exploited the Internet’s special aptitude for harvesting, sifting, and remarketing information about visitors, often surreptitiously, with little if any respect for the wishes of the individuals involved. On the other, awareness of these zero-privacy practices has led many consumers to develop an abiding distrust of “the Internet,” with consequent misgivings about disclosing personal data or doing business online.

Though concern about computers and privacy is nothing new, the Internet offers unique temptations both for collectors of personal information and for individuals who are asked to reveal it. A department store or mail order house may be able to deduce customer interests by tracking purchases, but on the Internet merchants can track not only what customers buy but also what else they look at and for how long. If the customer arrived at the merchant’s site in the usual way, via a hyperlink from a referring site, the merchant’s server logs will record the identity of the referring site, providing a source of additional clues about the customer’s interests or browsing patterns. Instead of relying on hit-or-miss surveys to

2 P. Sprenger, Sun on Privacy: ‘Get Over It’ WIRED NEWS (Jan. 26, 1999) <http://www.wired.com/news/politics/story/17538.html>. McNealy is the Chairman and CEO of Sun Microsystems, which is both the developer of the Java programming language used to implement applets in web browsers and a member of the Online Privacy Alliance.

3 Because similar personal information may be shared with a number of sites, and because there is a delay between the initial disclosure of information and the onset of such aggravations as unsolicited e-mail messages, the exact source of the privacy invasions is often hidden from the consumer. This disconnection between cause and effect can lead to a “one bad apple” syndrome whereby the actions of a small number of irresponsible websites may be attributed to the Internet as a whole.

4 Many of the privacy concerns and principles discussed in this article can be traced to a 1973 study by the DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, SECRETARY’S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS. According to a 1992 survey, over two-thirds of Americans believed that “the present uses of computers are an actual threat to personal privacy” and that “if privacy is to be preserved, the use of computers must be sharply restricted in the future.” Equifax-Louis Harris Consumer Privacy Survey, EQUIFAX EXECUTIVE SUMMARY 1992 ¶4 (visited Nov. 3, 1999) <http://www.privacyexchange.org/iss/surveys/eqfx.execsum.1992.html>.
assess the efficiency of advertising in bringing customers to the store, web merchants can receive a database-ready audit trail detailing which customers clicked on which ads on their way to the site. Combined with personal demographic information gathered in a registration or transaction process—or purchased from third parties—and analyzed with sophisticated data-mining and predictive programs, this information becomes a powerful marketing tool. The process is tempting not only because the data is so valuable, but also because obtaining it is so easy. Virtually every “dotcom” startup’s business plan includes a section on the site’s ability to construct and exploit demographic and psychographic profiles of visitors, blurring the “fine line between good service and stalking.”

For consumers, the temptations to disclose information are many, from the convenience of ordering products online, to the benefits of registered membership in a free community or portal site (such as user-defined content, public or private discussion forums, etc.), to the personalized buying suggestions, and even third-party advertisements, that arrive as a result of making one’s self known to a site. And again, it is so easy to disclose the information. The problem is that once the cat is out of the bag, it may be difficult to stop the resulting onslaught of marketing electronic mails (e-mails), savory and otherwise, and direct mail and telephone solicitations—especially if the website has shared the information with third parties.

As the web has matured into a mainstream business channel, the need to strike a more appropriate balance between business and consumer interests has become plain. The backlash of mistrust provoked by some websites’ cavalier treatment of personal information threatens to impede the growth of e-commerce, and so enlightened self-interest dictates that the business community focus on building consumer confidence in the web. Privacy policies have become the centerpiece of this effort.

---

1 This Orwellian-sounding term refers to an analysis of attitudes, interests and opinions as distinct from mere demographic data; such an analysis can bring improvement in predictive success.

6 Tara Lemmey, President of Narrowline (now Executive Director of the Electronic Frontier Foundation), quoted in Esther Dyson, Privacy Protection: Time to Think and Act Locally and Globally, RELEASE 1.0 (Apr. 1998) <http://www.edventure.com/release1/0498body.html>.
III. PRIVACY.COM?

Of course, adopting a privacy policy is not enough; to protect the public and the website, the policy must be followed. This lesson was driven home by the Federal Trade Commission’s (FTC) 1998 GeoCities\(^7\) enforcement action, a watershed event that exemplified both the grounds for consumer privacy concerns, and the government’s response to them. One of the ten most visited websites, GeoCities was a “virtual community” that hosted members’ home pages and provided other services such as free e-mail, clubs and contests to its 1.8 million members. The membership application requested both mandatory and optional personal information, and included options as to whether the member wanted to receive specified marketing information. The site also promoted a club and contests for children, participation in each of which required the child to submit personal information and to establish a GeoCities home page.

The website included statements assuring members that their personal information would be shared with others only in order to provide members the specific advertising they requested, and that optional registration information would not be disclosed without the member’s permission. Actually, the members’ information had been sold or rented to third parties who used it for other purposes, including targeted advertising.\(^8\) As to children, the FTC found that the website created the impression that GeoCities was collecting the contest and registration information, when in fact this was done by third parties hosted on its site.\(^9\)

These blunders gave the FTC the platform it needed to make a public example,\(^10\) and to put into practice its oft-stated views on how websites should handle personal privacy issues. The case settled with a consent order\(^11\) that prohibited GeoCities from misleading consumers about its data collection, use or disclosure practices, and from misrepresenting who was

---

\(^7\) In the Matter of GeoCities, a corporation, FTC File No. 9823015 \(<http://www.ftc.gov/os/1999/9902/9823015cmp.htm>\).

\(^8\) Id.

\(^9\) Id.

\(^10\) The FTC action and proposed settlement were first announced in early June 1998, in SEC filings in connection with GeoCities’ upcoming public offering that August. GeoCities, Corp., SEC Form S-1 Registration Statement (June 12, 1998) \(<http://www.sec.gov/Archives/edgar/data/1062777/0001017062-98-001328.txt>\).

collecting personal information. GeoCities agreed to post a privacy policy explaining what information is collected on the site, its intended use, what third parties might receive it and how the member could access the information and have it erased from GeoCities' computers. In addition, GeoCities was required to obtain express parental consent before collecting personal information from children, and to delete all information previously collected unless the parents agreed otherwise. The FTC's timing was politically astute: a week before the case was made public, the FTC had asked Congress to enact legislation protecting children's privacy online, before the GeoCities order was officially issued, Congress had passed the Children's Online Privacy Protection Act of 1998 (COPPA).

What is most legally interesting about GeoCities is that it is based entirely on misrepresentation. The FTC does not (except under COPPA) have authority either to require websites to post privacy policies, or to prescribe their content, but under Section 5 of the FTC Act, it has broad enforcement power over "deceptive acts or practices." If instead of saying one thing and doing another, GeoCities had made no promises at all, it might have avoided becoming the most notorious bad example in the history of online privacy.

IV. WHY VOLUNTEER FOR LIABILITY?

As GeoCities shows, from a strictly legal perspective McNealy's "zero-privacy" remark has much to recommend it as an eight-word privacy policy. As long as one is not catering to children, gathering information from European consumers, or in an industry where information practices are already regulated, the main source of liability exposure in this area is violating one's own policy, and the McNealy doctrine would be impossible

---

12 Regarding children's issues, a similar settlement was reached in May 1999 with Liberty Financial Companies; see In re Liberty Fin. Cos., FTC File No. 9823522 (agreement containing consent order), (visited Sept. 28, 1999) <http://www.ftc.gov/os/1999/9905/lbtyord.htm>.
16 In this instance "legal perspective" seems oxymoronic: despite what law school teaches, business is about much more than avoiding every possible risk.
17 See infra Part VI.F (discussing the EU Privacy Directive).
18 Industries with regulated information practices include healthcare, banking, video rentals, cable television, and telecommunications.
to violate. Why should any business volunteer for potential liability by publicly adopting a higher privacy standard? Quite simply, one can’t afford not to.

A. THE NEW CONFIDENCE GAME

Every web-based business has a stake in consumer confidence. Even brands that already enjoy solid reputations have an interest in avoiding any taint from consumer fear, uncertainty and doubt concerning the web as a whole. And despite the spectacular growth of e-commerce, much doubt remains. Credible studies indicate that concern for privacy is the number one factor keeping non-Internet users off the net,¹⁹ and less than a quarter of all web users have actually purchased anything online.²⁰

The obvious product of this distrust is that people avoid disclosing personal information by opting against online transactions and website registration.²¹ Less obvious but equally troubling for online marketers is the “garbage in” syndrome: in two recent surveys, over forty percent of Americans who registered at websites admitted to providing false information some of the time, mainly because of privacy concerns; the figure for European registrants was over fifty-eight percent.²² Meanwhile, the market has responded to user privacy concerns with a variety of products and services designed to provide anonymous surfing and to block meaningful tracking of browsing behavior.²³ The message to marketers is clear: if you want useful and accurate data, earn it by assuring consumers that you will use it appropriately.

---


²⁰ LOUIS HARRIS AND ASSOC., INC. & ALAN F. WESTIN, PRIVACY AND AMERICAN BUSINESS and PRICE WATERHOUSE, INC., E-COMMERCE & PRIVACY SURVEY (June 1998) <http://www.privacyexchange.org/iss/surveys/ecommsum.html> (stating that 23% of Internet users have purchased online, whereas the Business Week/Harris Poll put the figure at 22%).

²¹ See Online Insecurity, supra note 19 (finding that despite the benefits of registering at websites, 59% of Internet users never do).


²³ Examples of such products include anonymous proxy servers for browsing privacy and anonymous e-mail remailing services.
Posting a privacy policy can make an enormous difference in consumer confidence: in survey after survey, overwhelming majorities of net users say that privacy policies are important, or would matter to them in deciding whether to trade information for benefits, or would increase their Internet usage, or information disclosure. Moreover, as privacy policies become nearly universal, the implicit message of not posting a policy may be that one should be assumed a “data bandit” until proven otherwise.

Just as having no privacy policy can be a handicap, claiming the high ground with a conspicuously consumer-friendly policy can confer competitive benefits. People are especially sensitive about the release of their

---

24 Louis Harris & Assoc., Inc. & Alan F. Westin, supra note 20 (noting that 91% of net users and 96% of those who buy products or services online call privacy policies “important” or “very important.” For computer users who are not yet online, the figure was 94%).


26 See Online Insecurity, supra note 19 (finding that 62% of respondents would increase their Internet usage).

27 See id. (finding that 57% of respondents would increase their amount of purchases).

28 TRUSTe/Boston Consulting Group Consumer Survey (visited Oct. 8, 1999) <http://www.truste.org/webpublishers/pub_bottom.html> states that information practice policy statements make it two to three times more likely that a consumer will provide personal information to a website; 56% of users in the Business Week/Harris Poll, supra note 19, indicated that a privacy statement would make it more likely for them to register at a website.

29 Approximately 65% of commercial websites in March 1999 included some form of information practices statement, in contrast to only around 14% of commercial websites in the previous year. Further, virtually all of the top 100 sites include some information practices statement, with eighty-one sites boasting a more or less comprehensive privacy policy. The first figure is from Mary J. Culnan, Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission (Mar. 1999), which evaluated 361 “dotcom” sites selected randomly from the top 7,500 sites. The 14% figure is from Privacy Online, supra note 13, an FTC study of 1400 sites. While these two studies are not direct equivalents, the trend towards adopting privacy policies is undeniable. The data on the top 100 sites is from Professor Culnan’s study, Privacy and the Top 100 Sites: Report to the Federal Trade Commission (June 1999) sponsored by the Online Privacy Alliance. While these upbeat figures mask wide variation in adherence to recognized privacy principles, they all support the present point that a site without a policy increasingly stands out from the crowd.

information by the original recipient to unnamed others. Reacting to this sensitivity, many websites have adopted a black-box model that consolidates the marketing function for third-party products in the website so that consumers’ identifying information need not be shared with the third-party advertisers. The outside vendor may specify group demographics for the targeted consumers but will not have access to an individual’s information until an order is actually placed, and may not receive it even then. A website that goes out of its way to identify itself in plain language as the consumer’s privacy ally makes a powerful marketing statement—particularly if the contrast with competitors’ indiscretions is explicit. Consider these excerpts from a musical instrument retailer’s policy:

WHAT YOU DO WITH zZounds today IS NOBODY ELSE’S BUSINESS. And we promise to keep it that way. . . . Not all businesses respect their customer relationships like we do at zZounds. Many businesses, including other large music instrument retailers, are eager to share the information they have collected about you. Your trust and your privacy is for sale to the highest bidder. . . . This will not happen when you shop at zZounds.

Indeed, taking this idea one step further, a growing market niche has developed around the business model in which the website openly bargains for web users’ demographic and psychographic profiles in return for a promise of limited anonymity, coupled with the privilege of sending targeted

---

31 See Beyond Concern, supra note 30 (finding that sharing data with third parties was the most important criterion users evaluate in deciding whether to reveal information to a website).

32 Respond.com has even adapted the reverse-auction model as a “black box”; the buyer fills out a form specifying the desired product and the desired price, Respond.com sends an email with this information (absent the buyer’s identity) to its list of registered retailers, collects the replies and forwards them to the buyer. The buyer can then follow up with a vendor if she wants to accept its offer. The “middleman” feature not only preserves anonymity, it also enables Respond.com to collect its fees, which are based not on sales but on the number of e-mails to which the given vendor replies. See, e.g., (visited Sept. 29, 1999) <http://www.respond.com/overview/index.html> (providing an outline of the black-box-auction model).

advertising to the users. The message of companies such as Juno and MyPoints is: tell us what we need to know to send you ads that will interest you, and we will keep your data confidential. To the extent that the marketing actually reflects the user’s interests, advertisements will not be “junk mail” to the user, and they will be far more effective on a per exposure basis for retailers.

Finally, nothing undermines trust like a well-publicized betrayal. It has proven surprisingly easy for marketers, tightly focused on how information can be profitably used and sold, to misjudge (or be oblivious to) consumer reaction to new initiatives. Properly implemented, a privacy policy serves as an internal touchstone for a company’s consumer information practices. As the standard for evaluating any change in these practices, the policy can help inoculate against the kind of ill-considered strategies that create public relations meltdowns.

B. SEAL APPEAL

“Privacy Seal” programs such as those sponsored by TRUSTe or BBBOnLine may also win consumer confidence. Privacy counterparts to the Good Housekeeping and Underwriters’ Laboratories seals, these programs bring the credibility of third-party assessment, verification, and dispute resolution to a website’s information practices. These programs require adherence to certain minimum standards in areas such as notice of information practices, consumer choice as to secondary uses of the

---

34 Welcome to Juno (visited Oct. 25, 1999) <http://www.juno.com>. A recent Juno advertisement (targeted to online advertisers, rather than to consumers) states that “nearly 7 million Juno subscribers have filled out a member profile with more in-depth personal questions than your mother asks.”

35 See Welcome to The MyPoints Program (visited Sept. 29, 1999) <http://www.mypoints.com> (explaining that MyPoints participants are offered redeemable points—an Internet version of trading stamps—when they participate in MyPoints promotions or buy in response to MyPoints offers. A recent advertisement claims better than a 20% response rate to MyPoints e-mail advertising campaigns).

36 See, e.g., Alex Nash, Yahoo Retracts Unlisted Home Addresses, CNET NEWS.COM (Apr. 25, 1996), <http://news.cnet.com/news/0-1005-202-311165.html> (describing the consumer outrage and Yahoo’s rapid retreat when it was learned that Yahoo’s new People Search service disclosed some 85 million unlisted home addresses and telephone numbers).


39 A “secondary use” is a use of information for a purpose other than that for which it was originally disclosed, such as use in a direct-marketing campaign of a mailing address originally obtained for product shipment.
information and its transfer to third parties, consumer access to stored data, information security, and data integrity. Both organizations have special rules for sites targeted at children, consistent with those of COPPA.40

Both organizations require completion of self-assessment questionnaires that probe the site's information practices in great detail—a useful exercise for anyone preparing a privacy policy—and both impose strict license agreements and provide for ongoing compliance reviews.41 BBBOnLine adds a mandatory, structured dispute resolution mechanism.42 As of July 1999, TRUSTe had about 600 licensees, who together account for about one-third of all United States web traffic;43 BBBOnLine rolled out its privacy seal in March of 1999, with approximately 300 applications on file44 and by September had 127 sites enrolled.45

The potential of these seal programs to win consumer trust was illustrated by a 1999 survey in which web users were shown twenty-seven certification marks used online, and asked to pick the two marks they were familiar with that most increased their trust of a website.46 The BBBOnLine and TRUSTe marks were ranked second and third (behind only the Verisign symbol), with thirty-six percent of respondents ranking BBBOnLine47 in their top two, and thirty-one percent naming the TRUSTe symbol.

---


41 See BBBOnLine: Privacy Program Eligibility Criteria (visited Nov. 2, 1999) <http://www.bbbonline.org/businesses/privacy/eligibility.html> (covering requirements for BBBOnLine Privacy Seals); TRUSTe License Agreement Rev. 5.0, supra note 40 (requiring licensees to agree to particular and comprehensive rules before awarding Privacy Seals).

42 See BBBOnLine: Privacy Program Eligibility Criteria, supra note 41 (disclosing requirements to which a business must agree in order to qualify for a BBBOnLine Privacy Seal).


47 At the time, the BBBOnLine privacy seal program was not in effect; the seal in question was BBBOnLine’s Reliability Seal, which relates to business practices other than privacy, but it is probably safe to assume that the organization’s privacy seal would garner comparable responses.
For over four years the FTC has consistently encouraged industry self-regulation efforts such as these seal programs, which promise such benefits to the government as avoidance of the First Amendment issues that arise when the government attempts to control the flow of information, and conservation of limited government enforcement resources.48

C. GORILLA MARKETING

As mentioned above, even the most trusted brands have a stake in public confidence in e-commerce generally, and in privacy protection as one of its components. The "800-lb. gorillas" of the net are beginning to weigh in pointedly on the side of privacy policies. Recently the Internet's two largest advertisers, IBM50 and Microsoft,51 announced that they would no longer advertise on websites that did not post privacy policies. A week after the Microsoft announcement, Disney's Go Network, which includes Disney.com, Infoseek, ABCNews.com, and ESPN.com, raised the ante by declaring that they would neither advertise on, nor accept advertising from, sites lacking a comprehensive privacy policy.52

Similar pressures are being exerted by trade associations such as the Direct Marketing Association (DMA), which required its 3,600 members to adopt its "Privacy Promise"53 by July 1, 1999. This policy requires members to inform customers of their right not to have their personal information sold, rented or exchanged; to honor consumer requests not to be contacted again by the member or not to have their information shared with others; and to consistently use the DMA's contact-suppression lists of consumers who have informed the DMA that they do not wish to receive direct-mail or telephone


49 See Maryann Jones Thompson, Tech Firms Still Top List of Net Advertisers, THE INDUSTRY STANDARD (May 20, 1999) <http://www.thestandard.com/metrics/display/0,1283,894,00.html> [hereinafter The Industry Standard] (ranking advertisers for 1998; Microsoft was first and IBM second with combined advertising expenditures of $63.4 million).


52 Disney and Go Network Institute Comprehensive New Advertising Policy to Promote Industry Adoption of Online Privacy Standards (June 29, 1999) <http://www.info.infoseek.com/press/06-29-99_policy.html>. The Go Network is one of the top five websites, and The Industry Standard, supra note 49, ranked its constituent Infoseek as the sixth largest advertiser on other websites in 1998.

solicitations (an e-mail suppression list is planned as well). In addition, the DMA has created an automated privacy policy generator\textsuperscript{54} that can be used by its members or others to create a simple privacy policy. A number of other industry associations,\textsuperscript{55} particularly in the banking and consumer marketing fields, recommend model information practice guidelines to their members.\textsuperscript{56}

These “gorillas” are not proselytizing privacy wholly out of concern for individual rights or the credibility of the Internet; they see a bigger gorilla on the horizon. A political consensus on appropriate use of consumer information has arrived, and effective self-regulation (at the level of the individual company and of the Internet community as a whole) is probably the only way to head off federal privacy legislation, with its threat of inflexibility and bureaucratization. These companies know that the alternative to adopting a privacy policy is to have the government adopt one for them. The choice is not whether to volunteer for liability or to avoid it; the choice is whether to define one’s own standard or to accept whatever standard the political process may define. We turn now to the “Fair Information Practices” consensus, its history and its gradual transformation into law.

V. FAIR INFORMATION PRACTICES

The consensus approach to personal information privacy is a market-based model that allows consumers to participate in decisions on disclosure and use of their personal information, within a framework of data security and integrity. As articulated by the FTC,\textsuperscript{57} the elements of “Fair Information Practices” are notice, choice, access, security, and enforcement.

\textsuperscript{54} DMA will help you create your own Company’s Online Privacy Policy (visited Oct. 2, 1999) <http://www.the-dma.org/pan7/dmers7c1-policy.shtml>.

\textsuperscript{55} See Privacy Online, supra note 13, at 54 n.73 (listing 11 associations that submitted guidelines or principles for the FTC’s consideration).

\textsuperscript{56} See id. app. E (reporting the submitted guidelines).

\textsuperscript{57} Id. at 7-11. Many other organizations have modeled their recommended information practices on the FTC list. See, e.g., Online Privacy Alliance, Guidelines for Online Privacy Policies (visited Oct. 2, 1999) <http://www.privacyalliance.org/resources/ppguidelines.html> (including headings of notice, choice, access, and security); United States Department of Commerce, Elements of Effective Self-Regulation for Protection of Privacy (visited Oct. 2, 1999) <http://www.ecommerce.gov/staff.htm> (including headings of notice, choice, access, security, and enforcement).
A. NOTICE

Consumers are entitled to clear and accessible notice of a website's practices of collecting, using, and disclosing personal identifying information, before the information is collected. Notice is the foundation on which the other principles operate, and accordingly the notice should address matters such as who is doing the collecting, what data is being collected and how it is being collected, how the data will be used, to whom it will or may be disclosed, and the consequences of refusing to give the information. The notice should also discuss the website's policies on choice, access, and security.

B. CHOICE

Consumers should be offered choice as to how their information is used beyond the purpose for which it was initially provided (e.g., to gain access to website features or to complete a transaction). Choice may be "opt-in" ("click here if you would like to receive valuable information from carefully selected business partners") or "opt-out" ("click here if you prefer not to receive junk mail from total strangers"). "Opt in" offers the stronger privacy protection because it establishes a default rule against disclosure and use.

The most important choice points are those concerning secondary uses by the website gathering the information (such as inclusion in the company's targeted mailing lists) and disclosure of the information to third parties.

C. ACCESS

Consumers should have reasonable access to stored information about them \(^{58}\) and an opportunity to correct inaccuracies or to have the data deleted.

\(^{58}\) This simple requirement conceals difficult questions about the practicality and necessity of disclosing to a consumer such database-resident information as their clickstream records, or the inferences drawn from that data by use of analysis programs. Likewise, questions abound as to the obligation to disclose to consumers information about them that has been acquired from third-party sources.
D. SECURITY

Websites should take reasonable steps to protect the security of the data, both internally and vis-à-vis outsiders, and to ensure its integrity (freedom from alteration) and accuracy.

E. ENFORCEMENT

These principles must be enforceable to be effective. The appropriate enforcement apparatus and the minimum standard of what enforceability means are at the heart of a spirited debate over whether self-regulation is sufficient or whether additional federal legislation is needed. Undoubtedly, the FTC has pressed for universal adoption of privacy policies in part to bootstrap itself into GeoCities-style enforcement authority under section 5 of the FTC Act. Also, a key issue in the negotiations between the United States and the European Union (EU) over the EU Privacy Directive has been an EU requirement that enforcement include a right to money damages for those injured by privacy violations.

For young children, there is a codicil to the first three principles: Parents must receive the notice and exercise choice on behalf of young children, and parents should have access to the information on file about their children.

These five principles owe their current acceptance to both their considerable history and their flexibility. First presented in a 1973 study by the Department of Health, Education and Welfare, they soon became the framework for the Privacy Act of 1974. They were adopted as guidelines by the Organization for Economic Cooperation and Development (OECD) in 1980, and with some important refinements, formed the basis of the EU Privacy Directive. Lately, they have been strongly advocated by the Commerce Department and the FTC (the GeoCities order is a roadmap

---

59 The Online Privacy Alliance, a consortium of over 80 companies and associations involved in e-commerce, advocates that self-regulation via third party privacy seal programs is sufficient. However, they take pains to say that complaint-resolution processes of seal programs should not prevent the consumer from pursuing "other available legal recourse." Online Privacy Alliance, Effective Enforcement of Self Regulation (visited Oct. 3, 1999) <http://www.privacyalliance.org/resources/enforcement.html>.
60 See discussion infra Part VI.F (discussing the EU Privacy Directive).
61 See supra note 4 (discussing the 1973 study).
63 OECD, GUIDELINES FOR THE PROTECTION OF PERSONAL DATA AND TRANSBORDER FLOWS OF PERSONAL DATA (1980).
WEBSITE PRIVACY POLICIES

VI. THE LEGAL LANDSCAPE

Though America has recognized enforceable privacy rights in personal information for nearly a century, the legal context for website privacy policies is, for the most part, new and rapidly evolving. Drafting a privacy policy means navigating a variety of United States statutes and legal principles of relatively narrow scope—a situation that has been described euphemistically as a “sectoral” or “layered” approach and realistically as a “patchwork” or “minefield”—as well as anticipating where United States and EU law may be headed. Without attempting a complete analysis, this part highlights the major legal issues that impact formulation of a privacy policy.

A. PRIVACY TORTS

Although the common law of torts is not currently a major concern for the ordinary business practices of commercial websites, it cannot be ignored. The most relevant common law concept is invasion of privacy by public

---

64 As early as 1905, the Supreme Court of Georgia had recognized the right to privacy as against misappropriation of one’s likeness. Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 18 (1905).


disclosure of private facts. However, this cause of action arises only if the
information revealed would be highly offensive or humiliating to a
reasonable person, is of no legitimate public concern, and is disclosed widely
ever to be "substantially certain to become . . . public knowledge."

The case of naval officer Timothy McVeigh is a cautionary tale for online
businesses in this area (although it is by no means clear that the elements of
this tort were actually present in that case). A Navy investigator duped an
America Online (AOL) service representative into confirming that McVeigh
was the person behind an AOL user profile that listed the user as being gay; the Navy attempted to expel McVeigh from the service on that basis. For
AOL, which settled out of court, the incident uncovered a need to redouble
its staff education efforts on protection of members' privacy, including
"scenario training" aimed at helping customer service representatives deal
effectively with attempts to access member information via subterfuge.

Looking ahead, website operators should be alert for cases which may
lower the threshold of "public disclosure" in light of the ease of wide
dissemination of data over the web; but even if this occurs, the likelihood of
tort liability for disclosure of ordinary marketing information seems remote.
Sites that deal in especially sensitive information such as health status, mental
illness, emotional or family problems, and sexual matters are at greater risk.
Someday, someone who has ended up on a mailing list targeted at
participants in anonymous discussion forums on masochism, obsessive-
compulsive disorder, and Ivy League football is going to get mad enough to
sue, and just might win.

For purposes of this article, the most important feature of tort law is that
consent is a defense. In the tort context, it may be debatable whether
submitting information on a website constitutes legally binding consent to
the information practices stated in the website's privacy policy, but the
argument is at least plausible. Websites that deal with highly sensitive

68 Id. at cmr. a. This standard is seldom met in ordinary business transactions. For example, in
Tureen v. Equifax, Inc., 571 F.2d 411, 419 (8th Cir. 1978), Equifax's disclosure of the plaintiff's medical
underwriting history to her health insurer, at the insurer's request, was held not to be sufficiently "public"
for an invasion of privacy cause of action.
70 Philip Shenon, Navy and America Online Settle Case on Gay Privacy, N.Y. TIMES, June 12, 1998,
71 Id. In related litigation, the Navy was found to have violated both its own "don't ask, don't tell"
information, including those with anonymous or private discussion forums, typically have a click-wrap user agreement that can be integrated with the privacy policy to ensure valid consent.

B. THE FTC ACT

As the GeoCities discussion suggests, and the FTC seems to have publicly conceded, the FTC’s jurisdiction under the FTC Act is effectively limited to ensuring that a website’s practices mirror its stated policies, if any. Previously, the FTC staff had asserted that even if no promises are made to the user, some information practices might be “inherently unfair” in the context of collection and release of information from children, but this position seems moot in light of COPPA and is unlikely to be asserted as to data collected from adults. There is no private right of action under the FTC Act, so consumers seeking damages for privacy policy violations must find another theory of liability, such as contract.

C. COPPA

Enacted in October 1998, COPPA applies to commercial websites and online services that are targeted at children or that have actual knowledge that information is being collected from a child. It codifies the FTC’s Fair Information Practices as imposed in the GeoCities Consent Order, starting with the requirement of posting a privacy policy describing what information the site collects and how it uses and discloses that information.

---


74 See infra Part IX (discussing Contract Concepts).

75 Nonprofit organizations are exempt, just as they are exempt from the FTC Act.

76 E.g., by virtue of information entered in an “age” field in the data-collection screen.

77 COPPA, supra note 40, § 1303(b)(1)(A)(i).
The cornerstone of COPPA is prior "verifiable parental consent" to the collection, maintenance, and disclosure of information about children twelve and under. COPPA complements this initial parental "opt-in" with a continuing "opt-out" right to stop further use or collection of information from the child and also gives parents access rights to stored information. Exceptions to the "verifiable parental consent" requirement accommodate the practicalities of getting the consent in the first place (how would you know whose parent to contact or how to contact the parents, unless you ask the child?) and allow isolated e-mail contacts and actions necessary to protect the child's safety, to comply with the law, or to deal with website security issues.

Covered websites are prohibited from extracting extraneous information from children as a prerequisite for entering an online contest or other activity and are required to use "reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children." Finally, the law provides for a "safe harbor" whereby a website will be deemed in compliance with COPPA if it complies with an industry self-regulatory program approved by the FTC.

Enforcement of COPPA depends on the issuance of implementing regulations, which were due by October 1999; the only actual offense under the law is violation of the regulations. The proposed regulations, which have received extensive public comment, address such issues as defining when a website is "targeted at children," what is considered "personal information," and how to notify parents. Most important in this context, since the approved programs would have to mirror the requirements of the law and the underlying factual questions of compliance would be essentially the same with or without the safe harbor, it is not immediately obvious what substantive difference the safe harbor makes, but it does show a willingness by the government to outsource some of its compliance-enforcement work to industry groups, where the industry groups would no doubt prefer that it reside.

---

78 "Verifiable parental consent" is defined id. § 1302(9).
79 Id. § 1303(b)(1)(A)(ii).
80 Id. § 1303(b)(1)(B)(ii).
81 Id. § 1303(b)(1)(B)(i), (iii).
82 COPPA, supra note 40, § 1303(b)(2).
83 Id. § 1303(b)(1)(C).
84 Id. § 1303(b)(1)(D).
85 Id. § 1304. Since the approved programs would have to mirror the requirements of the law and the underlying factual questions of compliance would be essentially the same with or without the safe harbor, it is not immediately obvious what substantive difference the safe harbor makes, but it does show a willingness by the government to outsource some of its compliance-enforcement work to industry groups, where the industry groups would no doubt prefer that it reside.
86 Id. § 1303(a)(1).
the proposed regulations impose specific requirements for the content and placement of the website's privacy policy.

For most websites, the response to COPPA should be to avoid knowingly collecting information from young children, either by omitting age questions altogether or by providing data fields for age where 0-12 are invalid entries. These measures could be accompanied by a notice that the website does not wish to collect information from children twelve and under. For websites that actively cater to children, the law has ramifications not only for the privacy policy itself but also for site and database design. Like any privacy policy, COPPA sets a behavioral standard that the site operator must design its back-office systems to implement.

D. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)

Enacted in 1986 and hence not explicitly addressed to the web as it exists today, the ECPA provides both criminal penalties and civil remedies, including punitive damages, for unauthorized interception or disclosure of electronic communications and unauthorized access to stored communications.\(^8\) Parsing through the definitions reveals that the ECPA's reach may be greater than first appears. "Interception" means acquisition of the "contents" of a communication,\(^9\) and "contents" is expansively defined to include "any information concerning the substance, purport, or meaning of that communication."\(^90\) "Electronic communication" includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature,"\(^91\) a definition broad enough to encompass a browser request for a particular web page, the transmission of a cookie, and other browser-server interactions.

The ECPA has obvious application to the monitoring or disclosure of e-mails, or of discussions in private forums or chat rooms, by a site that provides those services. Presumably the statute's exceptions permitting interception and disclosure by "parties to the communication"\(^92\) exempt the

\(^9\) Id. § 2510(4).
\(^90\) Id. § 2510(8) (emphasis added).
\(^91\) Id. § 2510(12) (emphasis added).
\(^92\) Id. § 2511(2)(d).
collection, analysis, and disclosure of clickstream data by websites; however, in some contexts an argument could be made to the contrary.  

Exceptions also exist for interception and disclosure of electronic communications by third parties with the consent of a party to the communication. As with tort law, it may be unclear whether simply posting a privacy policy that warns of monitoring or disclosure will lead to a conclusive presumption of consent. Therefore, website operators contemplating monitoring or disclosure that might be questionable under ECPA should consider an auditable click-wrap consent.

E. FAIR CREDIT REPORTING ACT (FCRA)

The FCRA may apply to a website if it regularly collects and furnishes to others certain types of information that may be used for purposes such as credit or insurance underwriting, employment decisions, or deciding whether to enter into a transaction with the person in question. These “consumer reports” may be used only for limited purposes, which do not include the marketing of any products other than insurance and credit. Even for those two industries, consumers must have an opportunity to opt out of receiving unsolicited insurance and credit offers. An exception allows the use and reporting of one’s direct “transactions and experience” with the consumer. However, where a website merges its own data with data obtained from other sources and discloses the results, the exception would not apply.

---

93 Suppose a website, as a result of monitoring browser requests to its server, tags an individual as a regular participant in a closed forum on “Living with a Diabetic.” The explicit communication from the browser is merely to access a page with a particular address, and the website is a party to that communication with the presumptive right to disclose it. However, given the known subject-matter of discussions in the forum, does disclosure to a marketer of the nature of the page requested constitute an interception and disclosure of the broadly defined “contents” of the user's communications within the forum, communications to which the website operator is not a party?


95 See Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990) (finding that consent to the recording of telephone calls is presumed where the landlord informed a tenant that all incoming calls would be recorded). With privacy policies, the question is: what if the user claims not to have seen the policy?


97 15 U.S.C. § 1681a(d) provides that covered information includes information “bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.”

98 Id. § 1681b(3).
Especially relevant to website privacy policies are several provisions requiring express consumer consent to particular disclosures (e.g., disclosures in connection with employment decisions or medical information). Similarly, an exemption for disclosures to company affiliates applies only if the consumer was clearly and conspicuously informed of the possibility of such disclosures and had an advance opportunity to opt out.99

Because the requirements of FCRA are complex, interpretive problems abound, particularly as to the distinction between a regulated “consumer report” and an unregulated “marketing profile.”100 Accordingly, any website that reports consumer information obtained from third parties should evaluate its information practices to determine whether the statute applies. If it does, it will have a significant impact on the website’s information practices and privacy policy.

F. THE EU PRIVACY DIRECTIVE

The EU Privacy Directive sets minimum standards for personal information processing within the EU, and prohibits the transfer of this data to non-EU countries that do not provide “adequate” privacy protection.101 Because most European nations have had comprehensive privacy statutes for some time, the United States, with its ad hoc or “sectoral” approach, has not been recognized as providing adequate protection; negotiations designed to remedy this discrepancy are ongoing between the United States and the EU. In the meantime, transborder data flow continues, but ultimately change is in the wind for United States websites that collect personal data from Europeans.

99 Id. § 1681a(d)(2)(A)(iii).
100 This distinction is the subject of Trans Union Corp. v. FTC, 81 F.3d 228 (D.C. Cir. 1996), where the Federal Circuit held that targeted marketing lists were not necessarily “consumer reports” even though they were created from data originally gathered to be used in conventional credit reports, on the dubious grounds that the routine inclusion of this data in credit reports did not prove that particular data was actually expected to be used as a factor in credit decisions when it was collected. The court remanded to the FTC for further factual determinations, and an FTC Administrative Judge made the required factual determination and held Trans Union in violation of FCRA. In re Trans Union Corp., No. D-9255 (July 31, 1998) <http://www.ftc.gov/os/1998/9808/d9255pub.id.pdf>. Trans Union has appealed the order to the full Commission.
The EU and the United States are discussing a set of draft “Safe Harbor” principles\(^\text{102}\) that American companies could adopt in order to qualify their data protection practices as “adequate,” and in doing so ensure continued access to consumer data from Europe. In effect, the Safe Harbor in its present form measures “adequacy” largely in terms of conformity to the EU model.

The Safe Harbor standards are similar to the FTC Fair Information Practices, but include important elaborations on those principles. First, the EU considers data concerning union membership, religious and political affiliation, medical condition, sexuality, and racial or ethnic origin to be especially sensitive, and therefore requires an express “opt-in” before this information can be used for any purpose incompatible with that for which it was originally submitted. For all other personal information, there must be an “opt-out” opportunity to prohibit its use in marketing, either by the original recipient or by others to whom the data is transferred. When data is to be disclosed to third parties\(^\text{103}\) pursuant to a privacy policy notice (as opposed to transfers with the explicit consent of the consumer), the transferor must ensure that the recipient also follows the Safe Harbor rules. The EU also requires the availability of private money damages as an enforcement mechanism, while many in the United States have advocated that enforcement by expulsion from self-regulatory organizations or through government action under the FTC Act should be sufficient.\(^\text{104}\) Furthermore, there remain significant open questions about the appropriate extent of consumer access to stored information, especially where the information has been processed (e.g., preference databases extracted from clickstreams).\(^\text{105}\)


\(^\text{103}\) It would appear that under the EU Privacy Directive, affiliates of the collector of the information would be considered “third parties” if they are not processing the data on behalf of the collector, which would mean the individual must be given opt-out privileges to prevent proposed transfers to these affiliates. EU Privacy Directive, supra note 1, art. 2, §(f). The Draft Safe Harbor does not adopt the Privacy Directive’s definitions, however, and uses the flexible and undefined term “organization” to describe the collector of data.

\(^\text{104}\) United States Department of Commerce, Elements of Effective Self-Regulation for Protection of Privacy, supra note 57; Online Privacy Alliance, Effective Enforcement of Self-Regulation <http://www.privacyalliance.org/resources/enforcement.shtml>.

Besides these substantive differences from the FTC Fair Information Practices, a host of additional issues stem from the fact that the EU Privacy Directive is law and the FTC practices are not. Those who question whether self-regulation is really preferable to government prescription have only to look at the fastidious and rigid implementation by the EU of the broad principles that the Privacy Directive and the Fair Information Practices have in common.

Though the EU and the United States have not reached final agreement on the Safe Harbor, its outlines are definite enough to enable United States websites to conform their database structures and information practices to it, with the possibility of fine-tuning later. American websites will have to decide whether it is worthwhile to accept data from the EU at all, and if so, whether to partition one’s data and information practices according to national origin, or to allow the EU principles to govern one’s entire operation.

G. SECTORAL LAWS

As indicated previously, a number of narrow federal privacy laws apply only to particular industries or particular information, especially medical information.106 At press time, several comprehensive healthcare information privacy bills were pending in Congress,107 and the Health Insurance Portability and Accountability Act of 1996108 requires that the Secretary of Health and Human Services must issue regulations covering electronic storage and transmission of healthcare information. In addition, numerous state laws impose restrictions on the dissemination of various types of personal information, particularly health data.109 Other sector-specific federal

---


laws apply to information which could conceivably be gathered on a website but which is not, such as cable television subscriber records and video rental data.

Reflecting the explosive growth of online banking, the Office of Thrift Supervision, the Office of the Comptroller of the Currency, and the FDIC have all recently issued guidance to institutions under their supervision urging them to post privacy policies on transactional websites. For virtually all web-banking accounts, the Electronic Funds Transfer Act and implementing regulations already require financial institutions to inform customers of the institution’s policy on disclosing account information to third parties, including affiliates.

At this writing, H.R. 10, the Financial Services Act of 1999, is making its way through Congress with proposed provisions addressing the sharing of customer information with affiliates, telemarketers, and other third parties, and requiring specific disclosures about an institution’s privacy policy and consumers' options regarding the use of their personal information. In hearings on the bill, the FTC has testified that the sale by financial institutions of their direct “transactions and experience” data (which is exempt from FCRA) “raises serious privacy concerns.” The FTC has endorsed H.R. 10’s restrictions on disclosure of this information, and has called for stronger regulation of information-sharing with corporate affiliates.

transmitted and communicable disease clinical laboratory tests).

H. THE ONLINE PRIVACY PROTECTION ACT OF 1999

This bill is not yet law, and the FTC has stated that, as of July 1999, it may not be needed. But it is typical of the bills regulating privacy practices—the sticks to self-regulation’s carrot—that are regularly introduced and reflect, to varying degrees, the FTC’s Fair Information Practices. This proposal would require commercial websites to post privacy policies and to implement the principles of choice, access, and security—essentially COPPA without the special protections for children. Like COPPA, the bill delegates regulatory authority to the FTC and, for industries exempt from FTC jurisdiction, assigns enforcement responsibility to the appropriate federal regulatory agencies (e.g., the Comptroller of the Currency for national banks). This bill and others like it serve as a warning that any site currently avoiding Fair Information Practices merely because none of the existing laws apply to it may soon face the need to redesign its site, its practices, and its policies.

Because of the fragmented and overlapping quality of this loose collection of laws and the likelihood of equally fragmented, incremental change, it is generally impractical for a website to tailor its practices to applicable law as to each category of information. As a result, complying with the “highest common denominator”—the strictest rule applying to any information processed by the site—is usually necessary as to all information collected.

119 Federal Trade Commission, Self-Regulation and Privacy Online: A Report to Congress (visited July 21, 1999) <http://www.ftc.gov/os/1999/9907/privacy99.pdf> . While advocating continued monitoring of the progress of self-regulation and refusing to rule out the eventual need for online privacy legislation, the report concluded that “legislation to address online privacy is not appropriate at this time.” Id. at *12.
If adopting a privacy policy is “doing the right thing,” it is no less imperative to “do the thing right.” Two recurring points stand out in the discussion so far: first, a valid consent solves many problems; second, the key to avoiding liability is to have practice follow policy. With these principles in mind, and with an eye towards likely changes in one’s own organization, a website can seize control of the risks and define the terms of its covenant with the public. For a very simple website, this may not be difficult, but as websites increase in complexity and the boundaries between them become less distinct, implementing a bulletproof policy may not be as easy as it looks.

A. CAN’T WE JUST COPY A FORM?

Plenty of good privacy policies are available on the web for copying, and the TRUSTe and DMA sites will even generate a customized draft of a privacy policy based on one’s answers to a list of questions. Why not just pick one policy and be done with it? Comparing any two sophisticated policies, or one generated by TRUSTe and one by the DMA, shows why: they are different. A policy is functional only to the degree that it matches the business model and activities of the site, and deals with any special legal requirements that may apply. The permutations are as limitless as the creativity of website developers. And from a customer relations viewpoint, policy, practices, and the tone or personality of the notice may need to be tailored to the site’s target audience (remember the zZounds example?121).

The issues are complex enough that IBM has announced a new privacy policy consulting service, with basic workshops starting at $15,000,122 and privacy audits (including systems reviews) by Big Five accounting firms can easily run into six figures.123

121 See supra note 33 and accompanying text (quoting the zZounds website).
122 Jeff Partyka, IBM Advises on Online Privacy (July 16, 1999) <http://www.pcworld.com/pcwtoday/article/0,1510,11830.00.html>.
123 A. Lash, Privacy, Practically Speaking, THE INDUSTRY STANDARD (Aug. 2-9, 1999) <www.thestandard.com/articles/display/0,1449,563,co.html>. The article mentions three audits costing $200,000 or more, and one program that involves quarterly follow-up inspections at $20,000 per inspection. For the record, legal costs are an order of magnitude lower.
The way to create a policy that meets your site's distinctive needs is to use a process that ensures that all the relevant issues will be systematically addressed. Our recommended process includes four steps: (1) an Audit of current practices; (2) Goal Setting; (3) Policy Formulation, Drafting, and Site Design; and (4) Implementation and Maintenance. At each stage, participation and buy-in by each relevant constituency—marketing and sales, strategic planning, business development, information systems and website design, and legal—is critical. Experience suggests that none of these groups can reliably describe what the others are doing at any given time, much less predict what they will want to do or why; and hence any marketer who gives a proxy to the information systems department (or vice-versa) on issues of site design or policy probably deserves what they get. We will summarize the steps in this process and then return for a closer look at some important policy and drafting issues.

1. Audit. You can't formulate or document a policy unless you know exactly what your site does. Step one is to analyze how you collect, use, and disseminate information, both within your organization and with affiliates and other third parties. Every place information is collected and each way of collecting it—registration, contests, special offers, orders, mailing-list subscriptions, notification services and user customizations, as well as passive data-collection methods, such as cookies—needs to be catalogued, and the information collected should be identified.

Once identified, the information must be traced to its destinations, internal and external. The following questions should be answered: How is the data analyzed or combined with data from other sources? To whom is it available within your organization (including affiliates), and how are they authorized to use it? How do they actually use it? How do they plan to use it? It is helpful to divide the existing and anticipated uses for the data into primary uses (those necessarily incident to the purpose for which the information was collected), and secondary uses (those related to purposes different from those for which the information was collected).

With respect to primary uses, determine whether you outsource any portion of the function (such as order fulfillment or credit card verification).

124 The BBBOnLine privacy program requires disclosures of whether data gathered on the website is merged with data from other sources, since this data-matching can multiply both the original data's usefulness to the website and the sense of intrusion into the user's privacy. Better Business Bureau, Sample Privacy Notice (visited Oct. 4, 1999) <http://bbbonline.org/businesses/privacy/sample.html>.
If you do, you must determine whether there are appropriate restrictions on the outsourcing party’s use and disclosure of the data. Is data being collected that is not used, and if so, why? This is also a good time to evaluate the physical and technical means used to keep the data secure.

If data is shared with third parties for secondary uses, what are those uses, and is there a contractual prohibition against unrelated uses and further disclosure? Are there means for detecting unauthorized use, such as “seeded” names in the data? Do you have the right to remove a user from the third party’s list upon request? Are there contracts requiring you to continue to provide any of these parties with data for a specified time, thus limiting your flexibility to implement more conservative data practices?

As web pages become more elaborate and marketing and content partnerships more common, the boundaries within which a privacy policy applies may become indistinct. Therefore, you should review the site for co-branding or other joint marketing sections, frames of third-party content, and other third-party links where it may not be evident who is collecting the information. Then you should consider clarifying this by means of re-labeling, alerts, conspicuous links to the relevant party’s privacy policy, or a combination of these in order to clearly define your privacy “jurisdiction.” Where third parties are collecting data directly from your site (as opposed to your disclosing it to them), have you imposed contractual privacy rules in order to avoid guilt by association?

You should also search your site to locate all statements about the use of information collected or about privacy rights—especially isolated statements that should be folded into a comprehensive policy or eliminated altogether. One “rogue” statement can undo careful drafting elsewhere. Be alert, as

---

125 Compiling sensitive data just because it is available, with no particular use in mind, is inadvisable since there is no immediate benefit to having it and there is always a risk of inappropriate use or disclosure.
126 Seeding refers to the practice of inserting into a mailing list fictional or coded names with addresses that lead back to the party who compiled the list, to provide a practical means for that party to monitor the use of the list.
127 This may have been GeoCities’ problem—the statements cited by the FTC were not in a single, comprehensive privacy policy, but were scattered among its New Member Application Form, its Free Member E-mail Program web page, and one issue of its World Report newsletter. GeoCities, FTC Docket No. C-3850 (decision and order) (Feb. 5, 1999) <http://www.ftc.gov/os/1999/99/9823015d%260.htm>.
well, for statements that contradict one another. Last June, United Airlines (United) found itself in a public-relations nightmare on this score when users noticed that what the website’s privacy policy gave, the user agreement took away. Although the privacy policy pledged that United would not authorize any use of profile information except by the consumers themselves, the click-wrap “terms and conditions” statement said that by using the site, users gave their “express and unambiguous agreement”\(^\text{29}\) that they had “no expectation of privacy”\(^\text{130}\) resulting from the use of United’s services. Further, through the click-wrap agreement, users gave their “express and unambiguous approval”\(^\text{131}\) for United to use their personal information “for purposes of solicitations, promotions, and marketing programs.”\(^\text{132}\)

The audit phase concludes with an analysis of whether any special legal requirements apply as a result of any of three considerations: (1) the type of information collected (e.g., health status), (2) from whom it is collected (e.g., children or Europeans), or (3) how it is used or disclosed (e.g., credit reporting). This analysis lays the groundwork for decisions on how to comply with, or become exempt from, those requirements.

2. **Goal Setting.** The next step is to consider what you really want to do with the data and with your website in the foreseeable future. This step can be skipped if the site meets your needs, but most audits result in ideas for improvement. If the site will be redesigned, new business models adopted or data practices changed, the privacy policy must reflect or anticipate these changes.

The major issue is the role of information collection and disclosure within the overall business plan; the fact that this exercise concerns data does not mean that the goal must be to collect as much data as possible and to maximize its use and disclosure. Do you want to position your site as a “privacy ally,” to take a middle-of-the road stance, or to place emphasis on the other benefits your site offers, while maximizing your freedom to use consumer data? Could you win more business with less trouble by focusing on better customer service instead of emphasizing data mining? Are you

---


\(^{130}\) Id.

\(^{131}\) Id.

\(^{132}\) Id. At this writing, no explanation for how this occurred had been made public; it is entirely possible that the privacy policy was the later and more authoritative expression of United’s intent and that there was simply an administrative oversight in failing to conform the user agreement to it.
willing to make strong commitments, or is your goal to minimize any possible liability?

Redesigns must also pass the practicality test: do you have the technical ability and financial strength to implement a data-management system reflecting the new business model? A potential redesign could include adding tags indicating when information was first collected (to track which version of an amended privacy policy applies) and for what purpose the information was collected (to distinguish between primary and secondary uses for that data), or to segregate data on children or EU residents and process it differently. Likewise, if your business has both online and offline data harvesting operations but uses a single company-wide database, you must either apply the website privacy policy to all data, even that gathered offline, or tag data according to its origin and design your systems to process it accordingly. The cost of redesigning back office data structures can be startling and may far outweigh the benefits of a redesign that looks good on paper, especially if you are modifying a “legacy system” that was only recently installed. In that case, it may make more sense to scale back target-marketing ambitions and to adopt conservative data practices.

Finally, any redesign may reopen questions raised in the audit phase: would the new practices trigger special legal burdens, or require cooperation or new assurances from third parties to whom you disclose information?

3. Policy Development, Drafting and Site Design. With the goals defined, the next step is to map out in detail how the website will handle data, and to reflect that map in a privacy policy and a site and data structure design. Again, coordination and feedback among technical, marketing, legal and other constituencies as the design progresses are critical to keep policy and practice from diverging.

The threshold question is whether to join one of the “privacy seal” programs, since doing so will both drive the policy development process and circumscribe the available policy options. These programs have many advantages; in particular they instill confidence without a “need to read” the privacy policy itself. But they also impose additional start-up and maintenance costs and demand certain minimum disclosures and practices

---

133 One recent project that included a new “opt-out” database cost $250,000. Lash, supra note 123.
that may not be required otherwise. These programs have teeth; in addition to expulsion from the program for noncompliance, either BBBOnLine or TRUSTe could sue for breach of the promises in its licensing contract. Worse, a failure to comply with BBBOnLine’s dispute resolution mechanism may earn you a referral to the FTC. BBBOnLine may conduct an unscheduled inspection of your website, and TRUSTe uses technical means to detect any privacy policy changes you may implement. Be aware that these programs may also ratchet up their membership requirements from time to time.

Most other policy issues involve choosing how the site will implement Fair Information Practices, a subject discussed separately below.

4. Implementation and Maintenance. The final step is implementing the new policy and data practices. At this point, human factors may be even more important than technical measures such as testing the database, setting security parameters, and protecting against hackers. The greatest risk of unauthorized use or disclosure comes from employees, and the greatest risk with employees is not malevolence but ignorance. Employees should be trained on the substance and importance of the new policy and held accountable for misuse or improper disclosure. In some cases separate employee-directed policies may be needed to complement the online policy, especially in organizations where there are many sources of personal data other than the website. Where website data is shared with affiliates, both the policy (or contractual restrictions) and employee awareness efforts should follow the data. In general, the more consistent data policies are across such an organization, the less likely a catastrophic mistake becomes.

134 For example, both BBBOnLine and TRUSTe regulate use of personally-identifiable information obtained from persons other than the data subject. Further, as mentioned earlier, supra note 127, on children’s sites BBBOnLine requires either posting an alert when a link leads to another site where the same privacy rules do not apply, or avoiding altogether links to other child-directed sites that do not follow “core privacy standards.” Better Business Bureau, supra note 124.

135 It is intriguing to note that the BBBOnLine license agreement does not include a “no third-party beneficiary” clause, so conceivably a consumer—for whose benefit the program presumably exists—might be able to sue for damages under that agreement if it were advantageous to do so. Better Business Bureau, supra note 124.

136 Effective June 30, 1999, TRUSTe added to its license agreement new data security requirements and a requirement that consumers have the opportunity to correct inaccurate data. Additionally, a provision for mandatory opt-out for secondary uses and third-party disclosures was added effective August 30, 1999. Changes In TRUSTe License Agreements, TRUSTE REPORTER (Spring 1999) <http://www.truste.org/newsletter/spring99.html#02>.

Published by Digital Commons @ Georgia Law, 1999
Implementation may require establishing or amending contractual relationships with third parties. If the privacy policy gives assurances about third-party use of personal data, all existing third-party contracts should be reviewed for restrictions consistent with these assurances, and procedures should be in place to ensure imposition of privacy obligations in all new relationships with third-party users, including support contractors and outsourcers. Of course, if the data is valuable, contractual restrictions on use and further disclosure should be routine, though the “privacy” rubric may not be in evidence. Here the interests of the consumer and the collecting website are aligned because the former’s privacy is the latter’s confidential business information. Likewise, agreements for links or for framed or embedded third-party content may need to be modified to make sure that it will be obvious when a user has left your privacy policy’s “jurisdiction.”

Finally, management policies should require that any change to the website structure or data-entry screens, to the privacy policy, to third-party data sharing or partnering arrangements, or to the database structure or access rights, must be checked against the privacy policy considerations mentioned above (including legal review) and authorized by responsible executive management. If applicable, procedures should be established for notifying the privacy seal program of the change.

We turn now to a discussion of policy choices that must be made, and of some drafting opportunities and pitfalls.

VIII. SELECTED POLICY AND DRAFTING ISSUES: IMPLEMENTING FAIR INFORMATION PRACTICES

The easy generalities of fair information practices must ultimately give way to concrete policies. Here are some of the implementation issues to be considered.

A. NOTICE

A privacy policy should be conspicuous; if your policy is user-friendly, you want users to know it, and if your policy is aggressive, you don’t want

---

32. As with any legal drafting problem, there are legitimate questions as to just how detailed and specific a privacy policy should be, but implementing any policy requires more focus than the fair information practices formulations provide.
anyone to be able to claim they didn’t see it. Ideally, the home page, every data-entry screen, and every invitation for the user to e-mail information should include a prominent link to the policy. As to alerts or other signals that different policies will apply to linked sites and co-branded areas, a balance must be struck between the likelihood of user confusion in each case and design and clutter considerations. It may be useful to delegate this problem to the third parties involved.

In addition to the question of site boundaries vis-à-vis unrelated third parties, the notice should address the boundaries of the privacy policy as it relates to corporate affiliates, other operating divisions, and data gathered through sources other than the website.38

If you want to simplify your legal obligations by excluding data from sources like children or non-United States residents, or if access to parts of the site or special features is conditioned on disclosure of personal data, the notice should so state. If you match data submitted on the site with data from other sources to build a more complete profile, it may be appropriate to disclose this. Certainly, if the merged data is made available to third parties, this should be disclosed. If you intend to purchase supplemental data on consumers, bear in mind that doing so may require disclosing personal information (e.g., a list of names, social security numbers, or other unique identifiers) to the supplemental data vendor, and this will have to be disclosed in your privacy policy.

B. CHOICE

A major policy consideration is the extent to which user choice will be an all-or-nothing decision. For example, in order to register for special features on your site, must the user agree to secondary uses of the data submitted, or will you allow a user to register and veto secondary uses?39 It

38 See infra Part IX.D for a detailed discussion of these issues.
39 Both BBBOnLine and TRUSTe require that users be allowed to “opt-out” of disclosure of their information to third parties for secondary uses. While an “opt-out” is also required for secondary uses by the website operator, both seal programs allow the operator some latitude in defining what a “secondary use” is in the privacy policy. TRUSTe License Agreement Rev. 5.0, supra note 40, at § 4.A; BBBOnLine: Privacy Program Eligibility Criteria, supra note 41. The current EU Safe Harbor draft seems to offer similar flexibility. Draft Safe Harbor, supra note 102. The FTC’s formulation of the Choice principle suggests that consumers should always have a choice as to secondary uses. Privacy Online, supra note 13.
may make sense to vary your rule depending on whether the primary use mainly benefits the website or the user; it would be foolish to condition a product sale upon consent to secondary use and third-party disclosure because some sales will be lost as a result, but conditioning contest entries upon such consent is a different story. The rule could also be varied among different secondary uses. For example, allowing use of demographic data for targeted banner ads may be required as a condition of registration, but the user could be permitted to opt out of disclosure to third parties.

Another issue is opt-out versus opt-in choice. The former will yield the most data since data flow continues until the user takes steps to stop it; the latter is best if you want to be perceived as a privacy ally. Opt-in decisions need to be easily reversible.

"Consent" is another word for choice. Where applicable law requires user consent, you must decide whether to rely on the theory that an opt-out scheme affords "implied consent," or whether to require opt-in with an audit trail to be on the safe side. COPPA and the EU Privacy Directive foreclose this issue in some cases by requiring opt-in consent.

C. ACCESS

A key question is exactly what data the user will have access to, the main distinctions being among data collected on the website, data collected or purchased elsewhere, and preference or profile data derived through analysis of the first two. The H.R. 10 Financial Services bill explicitly excludes from its access requirements any data resulting from proprietary processing, while the proposed Safe Harbor under the EU Privacy Directive contains a similar but less robust exclusion. Companies with extensive operations outside of the website are well advised to make it clear that the policy’s access provisions apply only to data collected on the website. By making this clear, a company avoids the burdensome obligation to seek out and make available all data in the company’s possession concerning a particular consumer.
With respect to passively collected data such as cookie or log file data, the question is whether to grant access at all, since this data may not be comprehensible without further processing.

D. SECURITY

Policy questions as to security include how extensive your technical and human-factor security measures will be, and how much detail about those measures should be revealed to the public. An overly detailed description can both compromise the effectiveness of the security measures and unduly commit the website to these particular procedures.

E. ENFORCEMENT

What enforcement mechanisms will you allow or require users to pursue? The privacy seal programs impose their own requirements in this regard but do not limit other remedies for consumers. Limiting users’ options for enforcement may be both prudent and achievable, as we will see in the next section.

IX. CONTRACT CONCEPTS

A. IS YOUR PRIVACY POLICY A CONTRACT? ARE YOU SURE?

Considering enforcement leads to the question: what is the legal effect of a privacy policy? As between the website and the user, a privacy policy bears all of the earmarks of a contract, but perhaps one enforceable only at the option of the user. It is no stretch to regard the policy as an offer to treat information in specified ways, inviting the user’s acceptance, evidenced by using the site or submitting the information. The website’s promise and the user’s use of the site and submission of personal data are each sufficient consideration to support a contractual obligation. Under this analysis, users would have the right to sue and seek all available remedies for breach of the privacy policy, without the need for private rights of action under such regulatory statutes as the FTC Act.

The online economy leaves no doubt that user “eyeballs” and data have market value to most websites.
But for the website, this contract may be a net full of holes, one that the website may get caught in but the user may easily slip through. Many popular websites use contractual concepts by making statements such as, “By using this site you agree to our privacy policy,” or even riskier, “We may change our policy at any time, so check back here frequently; your continued use following the posting of a policy change constitutes consent to the new policy.” These statements are sometimes contained in a privacy policy accessible only through a tiny link at the bottom of the home page that can be found only by actively scrolling down the page. Any website that relies on the binding effect of such a “contract,” for example, by expanding its third-party disclosure of pre-existing customer data,¹⁴⁴ is treading on dangerous ground. In such a case there is no independent evidence that the user assented to this “contract.” In contrast, if the user wishes to enforce the contract, she has only to affirm that, in fact, she did read and accept the website’s offer to protect her information and relied on its assurances when she entrusted the site with her personal information.

Of course, in order to claim the benefits of this contract, the user would have to acknowledge having accepted it, and this gives the website an opportunity to turn contractual obligation to its advantage by including protective provisions. But relying on acknowledgment by the consumer as a condition precedent to a contract claim does not solve the amendment problem mentioned above (where the contract assented to was the original one), nor does it afford protection against tort liability or generate a legally reliable consent when one is required by law.

B. MAKING IT LEGAL

The more unavoidable the privacy notice, the less opportunity for a disgruntled user to claim that he did not see, read, or understand the privacy

¹⁴⁴ Notably, both BBBOnLine and TRUSTe require that a website apply to personal data the privacy policies that were in effect when the data was collected, effectively outlawing “bait and switch” privacy promises by their licensees. See BBBOnLine: Privacy Program Eligibility Criteria, supra note 41; Privacy Policy Assessment Questionnaire, Section E1 (visited Oct. 31, 1999) <http://www.bbbonline.org/businesses/privacy/assess-html.html>. Both the Eligibility Criteria and the Assessment Questionnaire are incorporated by reference into BBBOnLine’s Participation Agreement (visited Oct. 31, 1999) <http://www.bbbonline.org/download/license.PDF>. See also TRUSTe License Agreement Rev. 5.0, supra note 40, at Schedule A, § 4.F (for an additional example). However, these policies have not prevented some licensees from using the “implied consent to policy change” techniques outlined in this article.
policy. At a minimum, links to the privacy notice should be conspicuously placed next to data-collection “submit” buttons. But why not go a step further and ensure that a bilateral contract is in force? If a privacy policy is essentially a contract enforceable at the option of the user, there is no downside to making the contract mutual. The express assent manifested by a click-wrap agreement offers valuable opportunities for moderating risk.

Click-wrap contracts are regularly formed on websites. When a purchase is made, the user is typically asked to agree to terms and conditions, and sites that allow user postings such as discussion forums and chat rooms usually require member agreements as a condition of registration. By incorporating the privacy policy into a click-wrap user agreement, or turning it into one, the website can potentially limit remedies and damages, exclude consequential damages, provide for notice of and a right to cure any breach, require mandatory dispute-resolution mechanisms such as a negotiation-mediation-arbitration sequence, specify governing law and forum, shorten the statute of limitations, extract representations from the user (e.g., as to nationality or age), provide for contingencies through a force majeure clause, and create clear evidence of binding consents or waivers.

Given the minimal money damages likely to result from any given privacy breach and the probability that most consumer complaints can be resolved with a sincere apology and a promise to do better (or to delete the information), it is fair to ask whether a contractual privacy policy is overkill. The two-word answer is: class actions. In the context of the web, with its computerized user databases and instantaneous communication across a global network, a privacy-policy violation is more likely to involve 10,000 individuals than only one. Wherever individual damages are small, plaintiffs numerous, and fact patterns similar, class action attorneys will soon follow. And they are not interested in apologies or data deletions unless they can be translated into fee dollars.

---

145 BBBOnLine requires a link to the privacy policy on every page in which data is collected. *BBBOnLine: Privacy Program Eligibility Criteria, supra* note 41, §§ “Eligible Sites.” The proposed regulations implementing COPPA require similar notice on sites aimed at children. COPPA, Prop. Regs § 312.4(B).

146 Like shrink-wrap software licenses, click-wrap agreements have now received express judicial sanction. Hotmail Corp. v. Van Money Pie, Inc., 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. 1998).
In *Hill v. Gateway 2000, Inc.*\(^1\), the Hills brought a warranty and RICO claim against Gateway and managed to get it certified as a class action. The Gateway product had come with a shrink-wrap contract containing a mandatory arbitration clause, which the trial court refused to enforce. The Court of Appeals for the Seventh Circuit reversed, enforced the arbitration clause and nullified the class action certification. Since most arbitration rules do not accommodate class actions, an alternative dispute resolution clause such as that used by Gateway may effectively neutralize the class action threat.\(^2\)

Another advantage of a bilateral contract is that it can provide a meaningful mechanism for amendment, should it ever be necessary to change the privacy policy in ways that might be considered adverse to the user. The example given previously, where the site warns of unilateral amendments and advises the user to check in periodically, might be viewed as less overreaching if a user can be shown to have expressly agreed to it. Also, it seems very likely that amendments would be enforceable if accompanied by a prior e-mail to the user with an opportunity to opt out or delete his/her data rather than accept the change. Privacy expectations seem to be a one-way ratchet—the more users learn about corporate data practices, the more privacy they demand, and the more the legislative process grants privacy rights—but there are still many cases in which a user-unfriendly amendment might be desirable. Examples include situations where a privacy-oriented business model did not work, or where the website is acquired by another business with a different privacy policy.

C. DRAFTING TECHNIQUES

Whether or not a click-wrap agreement is adopted, contract drafting concepts such as coverage, clarity, caution and conciseness should be brought to bear on the privacy policy. The challenge is to be clear and concise, and to use plain language, without making overly broad or absolute promises. There is a difference between promising "your data is secure" and saying,


“we use industry-standard security measures to protect your data.” From the website’s point of view, the former cries out for a protective list of exceptions—the many ways security can be compromised—but the latter speaks for itself. Should you say, “Your data will never be released without your consent,” or “We will never authorize release of your data without your consent?” Perhaps it depends on how much you trust your systems, your security, and your employees. Confining promises to objective facts within the promisor’s control is the heart of the drafting art.

A second important consideration involves identifying the necessary exceptions to the privacy promise. In the preceding example, exceptions would be needed for release under subpoena, search warrant, court order, civil investigative demand, or other compulsory process such as civil discovery. A cautious drafter might also except disclosures necessary to protect the website’s rights or to prevent harm to other individuals; to identify persons who may be violating the law, the user agreement, or the rights of third parties; and to cooperate with investigations of purported unlawful activities. In some cases routine disclosures to regulatory agencies, such as bank examiners, may also be necessary. Some website owners believe that they cover all of these situations with the statement that they will never willfully disclose personal information without consent.

As this article illustrates, privacy policies divide naturally into two components: fairly simple principles and detailed implementation of those principles. The former tend to be reassuring, the latter stupefying. Many of the better privacy policies take advantage of this division by beginning with the reassuring general principles and referring the reader to a list of “Frequently Asked Questions,” or just an expanded discussion, for all of the details, qualifications, examples, explanations and exceptions.

D. EXAMPLE: BOUNDARY CONDITIONS

The drafting principles of coverage and of caution can eliminate many legal problems with privacy policies because both principles address the issue of consistency between the written policy and the activities that it describes. We close with an illustration: the issue of boundaries, of where the policy

---

149 The identification of persons anonymously posting either false information about a publicly-traded stock, or inside information, are examples of this exception.
applies and where it does not—an area where many privacy policies have
foundered and where many more are ticking time bombs.

Coverage means identifying every place where a user might mistakenly
assume that your privacy policy applies and preempting that false
assumption. Using the results of the audit and policy formulation phases, the
drafter would make clear who is collecting the data in co-branded or partner
areas and whose privacy policy applies, warn users about outward links and
framed third-party sites, and identify to what extent, if any, the site has
imposed privacy requirements on these third-party sites. The data-gathering
activities of banner ad cookies would also be mentioned and excepted.

A site that hosts third-party home pages under a common domain name
should certainly mention that those pages are not covered by the host
privacy policy, although this is seldom done. Some corporations maintain
multiple sites under similar brands or domain names, or linked to one
another as a network, but with different privacy policies. Since users would
tend to assume that a company’s sites would all share the same policy, the
drafter would need either to consolidate the policies or to identify the
different sites and warn the users that privacy policies may vary.
Outsourcers such as employee-leasing companies or web-hosting firms
should be mentioned, along with their coverage by the policy or by
narrower confidentiality agreements. And if a company wants to allow
affiliated entities to use its customer data, it may wish to define the
boundaries of its organization to include present and future affiliates at the
cost of having the policy apply to those as well. Last, a well-drafted policy
might exclude unrelated operations of the company or its affiliates and the
data collected by those operations.

The principle of caution looks to the future and anticipates change. The
boundaries of an organization may shift over time, and yet in an
environment where acquisitions and divestitures are announced daily, few
privacy policies provide for this possibility. Sharing information with a

\[150\] Under the Draft Safe Harbor, supra note 102, and the EU Privacy Directive, supra note 103,
affiliates may be considered “third parties” despite any attempt to characterize them otherwise.

\[151\] See Wendy Marinaccio, Privacy Advocates Blast DoubleClick Merger, CNET NEWS.COM (June 21,
outcry against the acquisition of a market research company by one of the web’s premier advertising
companies, allowing DoubleClick’s 1,300 advertising websites to potentially exchange data with Abacus’s
collection of 1,100 catalog companies). It is doubtful, of course, that any privacy policy provision would
have prevented this essentially political reaction.
new parent, its other subsidiaries, a merged entity, or an acquired entity is not only common, but may be essential to the viability of many business combinations and so should be expressly foreshadowed in the privacy policy. Likewise, it may be wise to reserve the right to disclose or duplicate the customer database in order to sell the assets of an operating division.

X. CONCLUSION

An effective privacy policy expresses a delicate balance of marketing, legal, technical, and customer-relations issues, and successfully implementing a policy for a complex site can be challenging. Following the process suggested here should result in a privacy policy and information practices that are mirror images of one another, enabling the website to offer privacy assurances with confidence and to manage confidences with assurance.