



PRIVACY

What Every Manager Should Know

Companies can't afford to ignore the fact that consumers are increasingly concerned about how businesses use their personal information

Susan C. Haller

At the Core

This article:

- Lists consumer concerns about privacy issues
- Discusses how privacy has become a competitive issue
- Gives key components of effective privacy policies

Just a few years ago, information privacy issues were not even on the radar screen for most companies. More recently, however, consumers have become more aware of the issue and more concerned about the potential misuse of information about them by both government and business. Other developments that have pushed privacy issues to the forefront include technological advances, increased media coverage of companies' privacy missteps, privacy-related litigation, and an increased focus on privacy in Congress and federal regulatory agencies, as well as in state legislatures and regulatory agencies.

The business community, recognizing privacy as a competitive issue and responding to the increased consumer awareness of the issue, has made privacy a top-level issue. Many companies that obtain, maintain, use, and disclose personally identifiable information about consumers (e.g., name, address, e-mail address, telephone number, Social Security number) have:

- posted privacy policies on their Web sites
- created chief privacy officer (CPO) positions
- increased employee awareness and training about the issues
- established self-regulatory initiatives
- taken other noticeable measures to shore up their privacy policies and practices

Without a doubt, privacy is now an issue about which every company that collects and uses personally identifiable information about consumers should be concerned. Public and consumer concerns, as well as the rising volume of legislation and regulations, are such that all managers would be well advised to consider them.

What the Public Thinks

Consumers' interest in and concern about potential threats to their privacy have been measured in numerous polls and surveys. These indicate that consumers' privacy concerns have increased, especially over the past decade. In a 1999 survey conducted by the *Wall Street Journal* and NBC News, individuals were asked to identify the issue(s) that concern them the most about the 21st century. Remarkably, 29 percent of those participating in the poll responded that they were more concerned about threats to personal privacy than about other social issues, including overpopulation, war, and global warming.

Increased public concern about privacy has affected consumer decisions about which companies they are willing to do business with and what personal information they are willing to provide.

The increased levels of concern about privacy have been attributed to two factors: distrust of institutions and fears about the misuse of technology.

Undoubtedly, the events of September 11, 2001, have had a profound effect on the public's concerns about social issues, including privacy. Since then, Americans have expressed greater support for expanded law enforcement programs (e.g., increased surveillance) — a marked change in public opinion — even if the increased law enforcement powers would affect individuals' civil liberties.

In the online world, consumer concern about privacy has had a profound impact on e-commerce. For example, an October 2001 report by Forrester Research found that \$15 billion of projected 2001 e-commerce revenues could be unrealized because of consumers' concerns about their privacy. Among the key issues about online shopping identified by consumers are credit card number theft and the misuse of their personal information.

These figures demonstrate that companies cannot ignore the importance of privacy to consumers. Companies that fail to address privacy issues are likely to see an impact on their business.

The Role of the Media

Media reports about companies' privacy missteps have become not only front-page business section stories but true front-page stories as well. This media scrutiny has heightened public awareness of the privacy issue and, in some cases, resulted in legislative and regulatory activity.

For example, in 1999 the plans of a New Hampshire company, Image Data, to purchase drivers' photographs from state departments of motor vehicles and create a database of digital photographs that retailers could use to combat fraud were met with an immediate negative public reaction. Headlines, for example, raged "Your Driver's License, For Sale?" The public reacted strongly despite the fact that the law did not prohibit this practice, and Image Data offered consumers an opportunity to opt-out or have their photographs removed from the database.

Elected officials in several states acted quickly to halt the practice of allowing companies to purchase driver's license photographs. At the federal level, language was added to the FY2000 Transportation Appropriations Act to amend the 1994 Driver's Privacy Protection Act, the statute under which drivers' information had been made available for commercial purposes. Image Data ultimately changed its business plan for its database to a consent-based model where participating businesses scan the driver's licenses of consenting consumers only.

Also in 1999, the plans of Internet advertising company DoubleClick to purchase direct marketing company Abacus Direct, which housed the nation's largest catalog database, were well covered in the press. This purchase would have allowed DoubleClick to marry information about consumers' online habits (clickstream data) with Abacus' information, thereby creating personally identifiable online profiles and allowing DoubleClick's customers to better target online ads to consumers. (**Editor's Note:** Also see article by Cannon, page 42.)

Shortly after DoubleClick's plans were announced, the Electronic Privacy Information Center, a Washington, D.C.-based privacy advocacy group, filed a complaint with the

**Companies
that fail
to address
privacy
issues are
likely to see
an impact
on their
business.**

Federal Trade Commission (FTC) alleging that DoubleClick violated Section 5 of the FTC Act prohibiting unfair and deceptive trade practices. The FTC began an investigation, as did various state attorneys general, and in March 2000, DoubleClick backed away from its plans.

An attempt by failed Internet toy retailer Toysmart.com to sell personally identifiable information about its customers in violation of its privacy policy also received significant media attention. In May 2000, after filing for bankruptcy, Toysmart planned to sell its assets, including its customer list containing information about 250,000 customers. The Toysmart privacy policy, posted in September 1999, indicated that the company would never disclose customers' personally identifiable information to third parties. The FTC filed suit against Toysmart to prevent the sale of the customer list. More than 40 state attorneys general intervened in the bankruptcy proceedings.

A settlement was finally reached when Toysmart agreed to destroy the customer list and Toysmart's parent, Walt Disney Company, paid creditors \$50,000 to end the controversy.

Repeated stories about identity theft also have received significant media attention, some because they involve stealing the identity of celebrities and others because of the elaborateness of the identity theft scheme.

The Private Sector's Reaction

The private sector has reacted in a variety of ways to the emergence of privacy as a competitive issue. While the business community recognizes the need to protect consumer privacy, it also depends on access to consumer information to facilitate transactions, such as mortgages and car loans.

Privacy issues are no longer limited to industry sectors that have traditionally focused on them, such as the financial and medical sectors. Now any company that handles personal information about consumers should have a privacy policy and privacy practices in place. The expanded commitment to privacy has manifested itself in many ways, such as the creation of the CPO position. (**Editor's Note:** Also see article by Pemberton, page 57.)

According to *Business Week Online*, by the end of 2000 between 50 and 100 com-

panies had appointed CPOs, including IBM, American Express, Kodak, and Microsoft. The number had more than tripled by November 2001, according to *Information Security* magazine. Professional associations, such as the Association of Corporate Privacy Officers and the Privacy Officers Association, began to form shortly after the emergence of the CPO position. These two trade associations have now merged to form the International Association of Privacy Officers (www.privacyassociation.org).

Industry also has increased privacy protections through the establishment of self-regulatory organizations. One of the

According to Business Week Online, by the end of 2000 between 50 and 100 companies had appointed CPOs.

earliest such organizations was the Individual Reference Services Group, or IRSG (www.irsg.org). Established in 1997 and comprised of 14 leading information industry companies, the IRSG, in conjunction with the FTC, created self-regulatory principles for the dissemination and use of personal information. In September 2001, IRSG members decided to dissolve the organization due to the regulation of the information governed by the IRSG principles (e.g., Title V [privacy] of the Gramm-Leach-Bliley Act [financial modernization]).

Another industry self-regulatory group to rise out of

the emergence of the privacy issue is the Online Privacy Alliance (OPA), a coalition of more than 80 companies and organizations dedicated to online privacy protection (www.privacyalliance.org). OPA created guidelines for online privacy policies (i.e., notice and disclosure, choice/consent, data security, and data quality and access), and for enforcing self-regulation (e.g., verification and monitoring, complaint resolution, and education and outreach).

U.S. Privacy Protections

Privacy protections available in the United States can be traced back to three main sources: constitutional law, statutory law, and common law (e.g., public disclosure of private facts; breach of an implied contract; and misappropriation of name or likeness). In recent years, the business community has focused on enacting privacy statutes and promulgating regulations implementing these statutes. In the United States, privacy statutes have been enacted on a sector-by-sector basis. For example, Congress has enacted legislation regarding children's online privacy, driver's privacy, financial privacy, and medical privacy.

Children's Online Privacy. In 1998, Congress enacted the Children's Online Privacy Protection Act (COPPA) in an effort to give parents more control over the collection of personal information from children online. Beginning on April 21, 2000, COPPA required Web sites directed toward children under age 13 or sites that knowingly collect personal information from children to meet certain requirements, including:

- posting a privacy notice addressing specific issues such as type of personal information collected, how the Web site will use the information, whether the site operator will disclose the information to third parties, and how parents may contact the operator

- obtaining verifiable parental consent before collecting, using, or disclosing personal information from a child (certain exceptions include Web sites responding to a one-time request from a child)
- providing parents with an opportunity to review personal information that the Web site collected from their children
- allowing parents to revoke their consent and request that the Web site operator delete information collected from their children

COPPA allows children's Web sites to meet these requirements by complying with approved industry self-regulatory guidelines. The FTC, the federal agency responsible for promulgating the regulations implementing and enforcing COPPA, has approved three "safe-harbor" applications, including those of the Children's Advertising Review Unit of the Council of Better Business Bureaus Inc., ESRB Privacy Online, (a division of the Entertainment Software Rating Board), and TRUSTe. The FTC has taken an active role in educating the public and Web site operators about COPPA requirements. The Commission hosted two COPPA workshops — one before COPPA became effective and one after to address compliance issues.

Approximately one year after the effective date, the Center for Media Education (CME) issued a report, "Children's Online Privacy Protection Act (COPPA) — The First Year," on Web site compliance with COPPA. There had been concern that sites would comply with COPPA by reducing or eliminating online children's activities rather than meeting all of the requirements. CME found, however, that while COPPA had a significant effect on many of these Web sites' marketing and other business practices, many were able to meet the requirements without reducing or eliminating their sites' interactive features. CME reported that compliance issues did arise, however, with respect to the following COPPA requirements:

- A majority of affected sites did not display their privacy policies with a clear and prominent link.
- Many sites were not properly meeting the verifiable parental consent requirements.
- In an effort to ensure that children under 13 do not provide personal information, some Web sites use methods of verifying age that actually encourage age falsification.

Driver's License Information. In 1999, following Image Data's attempts to purchase drivers' photographs from state departments of motor vehicles (DMVs), Congress enacted amendments to the Driver's Privacy Protection Act (DPPA) to further restrict the entities to whom driver's license information may be disclosed. Effective June 1, 2000, the amendments prohibited state DMVs from disseminating drivers' photographs, Social Security numbers, or medical or disability information without first obtaining the drivers' expressed consent.

Certain exceptions to this general probation applied (e.g., dissemination to a government agency; to a court or self-regulatory

**All companies that
obtain, maintain,
use, and/or disclose
personal information
about consumers should
adopt a privacy policy.**

ry body; for use by an insurer or an insurance-support organization or self-insurer for claims, antifraud, rating, or underwriting purposes; or to an employer or insurer in connection with a commercial driver's license).

The legislation amending the DPPA replaced the existing "opt-out" system for individual look-ups and bulk distributions of personal information for surveys, marketing, or solicitations with an "opt-in" system. The amendments severely restricted driver's license information as a source of information for individual look-ups and for surveys, marketing, or solicitations because many states chose not to change to an opt-in system or for those states that did change, few individuals opted in.

Personal Information Obtained by Financial Institutions.

The collection, use, and disclosure of personal information by financial institutions also has been a focal point for privacy protection. During the 106th Congress, financial modernization legislation known as the Gramm-Leach-Bliley Act (GLB Act) included privacy protections (Title V). Beginning July 1, 2001, the GLB Act required financial institutions to provide notice and an opportunity to opt-out of disclosures of "nonpublic personal information" to nonaffiliated third parties (exceptions apply). Reaction to the GLB Act has been mixed. Consumers have been inundated with privacy notices, and many have complained that the notices are difficult to understand, according to a 2001 Harris Interactive survey.

In response to these concerns, the FTC, along with the seven other federal regulatory agencies responsible for implementing and enforcing the GLB Act, hosted a public workshop in December 2001 entitled "Get Noticed: Effective Financial Privacy Notices." The purpose of the workshop was twofold: to discuss concerns that have been raised about the clarity and effectiveness of the GLB notices and to provide guidance to financial institutions regarding the form and content of their GLB notices.

Almost immediately after the enactment of the GLB Act, legislation further restricting the release of personal information collected by financial institutions was introduced, including legislation to restrict the sharing of personal information among financial institutions' affiliates.

Health Information Privacy: In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). Under HIPAA, Congress had until August 21, 1999, to pass comprehensive health information privacy legislation. Congress did not meet this deadline and, as a result, the Department of Health and Human Services (HHS) was required to promulgate health information privacy regulations. These regulations took effect on April 14, 2001, and most entities covered by the regulations must be in compliance by April 14, 2003.

The HIPAA privacy rule requires covered entities — health plans, healthcare clearinghouses, and certain healthcare providers (e.g., those who conduct billing and electronic fund transfers) — to provide certain privacy protections, including:

- written explanations to patients regarding how their health information may be used and disclosed
- patient access to their medical records
- patient consent as a precondition to sharing health information for treatment or payment purposes
- a separate authorization for non-routine disclosures of health information for purposes that are not healthcare related
- patient recourse (e.g., formal complaint process) for privacy violations

Covered entities must also meet privacy safeguard standards.

Current Privacy Legislative Initiatives

Privacy legislation continues to be an area of interest for the 107th Congress. During the first session, proposals related to the following privacy issues were introduced:

- financial privacy
- online privacy
- Social Security number privacy
- identity theft
- unsolicited commercial e-mail (spam)
- wireless communication privacy/location
- the establishment of a privacy commission
- general/omnibus privacy
- student privacy
- health information privacy and genetic nondiscrimination
- do-not-call registries

Multiple congressional committees have jurisdiction over privacy-related issues, including the House and Senate Judiciary Committees; the House Financial Services Committee and the Senate Banking Committee; the Senate Commerce Committee and the House Energy and Commerce Committee; and the House Ways and Means Committee.

During the 107th Congress, the Subcommittee on Commerce, Trade and Consumer Protection of the House Energy and Commerce Committee has held a series of six privacy-related hearings. The chairman of the subcommittee, Rep. Cliff Stearns (R-Fla.), has also drafted an outline for a privacy bill that would cover both online and offline collection, use, and disclosure of personally identifiable information. The Stearns outline, proposing comprehensive privacy legislation, is a departure from the current U.S. system of providing sector-specific statutory privacy protections and includes the following key elements: pre-emption; privacy notice requirements; consumer choice requirements; security requirements; protections against identity theft; protections against Social Security number misuse; an international provision; and a workplace monitoring (e.g., electronic mail, Internet usage) provision.

Current Privacy Regulatory Initiatives

The FTC has become the de facto *federal privacy regulatory* agency. In 2001, Timothy Muris was appointed chairman of the FTC. In October 2001, he outlined his privacy agenda. Under Muris, the FTC is focusing on enforcing existing law protecting consumer privacy. He has pledged to increase the FTC's focus on enforcing current privacy statutes with a 50 percent increase in the FTC's enforcement resources. Currently, Muris is not recommending that Congress enact online privacy legislation. At a November 2001 hearing, Muris indicated that his position on this issue could change depending on whether the states begin to enact online privacy legislation.

FTC officials continue to provide further details regarding their privacy agenda. For example, during a December 2001 appearance at the Promotion Marketing Association's annual meeting, Howard Beales, director of the FTC's Bureau of Consumer Protection, stated that the FTC has adopted the position that a privacy policy posted on a company's Web site will be applied to offline privacy practices unless the company explicitly states in its online policy that it applies only to online activities.

Key Components of Effective Privacy Policies

All companies that obtain, maintain, use, and/or disclose personal information about consumers should adopt a privacy policy. When adopting such a policy, it is critical for companies to state what their information practices are and follow their stated privacy policies. Companies may find themselves in trouble and the subject of an FTC action or a lawsuit if their privacy policies do not accurately reflect their practices or if they violate their own stated policies.

The key components of a privacy policy are

- *Notice* - A company should provide consumers with a clear and conspicuous notice regarding its information practices, including those described below.
- *Consumer Choice* - A company should provide consumers with an opportunity to decide (e.g., opt-out) whether it may disclose personal information about them to unaffiliated third parties.
- *Access and Correction* - Companies should provide consumers with an opportunity to access and correct personal information that they have collected about the consumer.
- *Security* - Companies should adopt reasonable security measures to protect the privacy of personal information. These measures may include administrative security (e.g., access rules for employees and contractors), physical security (e.g., placing computer equipment in secure areas), and technical security (e.g., passwords and firewalls).
- *Enforcement* - The company should have in place a system by which it can enforce its privacy policy. Some companies rely upon independent third parties to ensure compliance. For example, some companies have obtained privacy seals from BBBOnLine or TRUSTe, both of which require participation in their consumer dispute resolution program and enforcement mechanisms.

Because privacy has become a competitive issue, companies should also be aware of and comply with industry-best practices to ensure that they are meeting industry standards — even those not required by law.

Companies also may want to offer consumers privacy protection through the adoption of various technological tools. For example, one of the technology standards that has emerged recently is the Platform for Privacy Preferences (P3P). P3P is a system for matching consumers' online privacy preferences with the privacy practices of participating Web sites.

Privacy is an area of constant, growing activity. To reduce the risk of a lawsuit, an agency action, or a negative news article, companies that obtain, maintain, use, and/or disclose personally identifiable information about consumers must dedicate the appropriate level of resources and personnel necessary to ensure that they comply with the applicable legal requirements and industry best practices. ■

Susan C. Haller, Esq., is an associate with Mullenholz, Brimsek, and Belair law firm in Washington, D.C., and a legal editor of Privacy and American Business. She may be reached at haller123@aol.com.

References

- “Children’s Online Privacy Protection Act (COPPA) — The First Year.” Available at www.cme.org (accessed 10 April 2002).
- “FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Operators.” Federal Trade Commission. 10 July 2000. Available at www.ftc.gov (accessed 10 April 2002).
- Hunt, Albert R. “Americans Look to 21st Century with Optimism and Confidence.” *Wall Street Journal*, 16 September 1999.
- Kelley, Christopher M., Alanna Denton, and Resa Broadbent. “Privacy Concerns Cost eCommerce \$15 Billion.” Forrester Research, September 2001.
- Kontzer, Tony. “FTC Spreading Its Privacy Net.” *Information Week*, 11 December 2001. Available at www.informationweek.com (accessed 10 April 2001).
- Krebs, Brian. “Online Privacy Policies Apply to Offline Data Practices.” *Newsbytes*, 10 December 2001. Available at www.newsbytes.com (accessed 10 April 2001).
- McCormick, Gavin. “Judge Approves Toysmart Deal.” *Boston.internet.com*, 30 January 2001.
- McCormick, Gavin. “Settlement Reached in Toysmart Case.” *Boston.internet.com*, 12 January 2001.
- McCullagh, Declan. “Your Driver’s License, For Sale?” *Wired News*, 1 July 1999.
- Mendels, Pamela. “The Rise of the Chief Privacy Officer.” *Business Week Online*, 14 December 2000.
- Parker, Pamela. “DoubleClick Drops Controversial Plan.” *Business News Archives* online, 2 March 2000. *Privacy & American Business*, 3 October 2001. Alan F. Westin. Available at www.pandab.org (accessed 10 April 2002).
- “Privacy Notices Miss the Mark with Consumers.” Privacy Leadership Initiative survey summary. Harris Interactive. December 2001.
- Rodger, Will. “DoubleClick Backs Off Web-Tracking Plan.” *USA Today*, 7 June 2000.
- Roiter, Neil. “The CPO.” *Information Security*, November 2001. Available at www.infosecuritymag.com (accessed 10 April 2002).
- Weiss, Murray. “How NYPD Cracked the Ultimate Cyberfraud.” *New York Post*, 20 March 2001.
- Westin, Alan F. Written testimony before the Subcommittee on Commerce, Trade, and Consumer Protection of the House Energy and Commerce Committee, 8 May 2001.
- “Woods’s Identity Thief Gets Maximum Sentence.” *GolfLine*, 28 April 2001.