

YOUR ONLINE PRIVACY POLICY

An informational paper about drafting your first privacy statement or improving your existing one.

reviewed by

TRUST·e
site privacy statement

© 2004 TRUSTe. All rights reserved.

Contents

- 2 What is a Privacy Statement?
- 3 Why Post a Privacy Statement?
- 6 Who Creates a Privacy Statement?
- 9 What does a Privacy Statement Cover?
- 12 What are Consumer-Friendly Privacy Practices?
- 14 Consumer-Friendly Privacy Statements
- 16 Privacy Resources
- 17 Sources

“Crafted correctly, your privacy statement is a meaningful communication that can build consumer trust and confidence. This trust will help protect your brand and its underlying promise from the ravages of the highly competitive online marketing space.”

Bennie Smith, chief privacy officer, *DoubleClick*

What is a Privacy Statement?

A privacy statement is a communication to consumers about how a company uses their personal information. Although businesses of all sorts create privacy policies, this paper focuses solely on public-facing privacy statements posted online. These statements are unique in that they are wholly public: they can be viewed by anyone, at any time, and apply to anyone visiting the Web site on which they are displayed.

Privacy statements reflect the unique data-handling practices of their respective Web sites.

Privacy statements come in many shapes and sizes. There is no current industry standard in the online community about what privacy statements should look like. Some take the form of lengthy, downloadable PDFs while others are simple disclaimers presented in a one-paragraph pop-up window. Every Web site is unique and a privacy statement must reflect a site's unique data-handling and collection practices.

The Federal Trade Commission's Fair Information Practices are the closest thing the industry has to an online standard for privacy practices. The Fair Information Practices are based on the principles of full disclosure that underlie an enlightened democracy. Specifically, only when consumers have a full understanding of how an organization maintains and uses information can they make informed decisions regarding the disclosure of their personal information.

The FTC's Fair Information Practices are the closest thing the industry has to an online standard for privacy practices.

The Fair Information Practices

- **Notice.** Web sites should provide full disclosure of what personal information is collected and how it is used.
- **Choice.** Consumers at a Web site should be given choice about how their personal information is used.
- **Access.** Once consumers have disclosed personal information, they should have access to it.
- **Security.** Personal information disclosed to Web sites should be secured to ensure the information stays private.
- **Redress.** Consumers should have a way to resolve problems that may arise regarding sites' use and disclosure of their personal information.

Why Post a Privacy Statement?

Privacy statements build consumer confidence. A privacy statement signals to consumers that a site respects their privacy concerns and has taken the time to evaluate its privacy practices and institute procedures to protect personal information.

Consumer attitudes toward privacy issues have become tougher in recent years. Studies reveal that fewer people trust businesses to handle consumers' personal information in an acceptable way. At the same time, fewer people put faith in existing laws to provide reasonable levels of privacy protection.¹

Privacy statements help to allay consumer anxieties significantly. More than 80 percent of online consumers have read a site's privacy statement and the remaining percentile report that even a short summary of a site's privacy practices make them feel more secure online.²

Privacy statements help consumers make more informed choices.

When consumers believe a site is trustworthy, they are more likely to engage in valuable online activities, such as making purchases, clicking on ads, disclosing personal information, filling out surveys for market research, contributing content, downloading software, and returning to the site in the future.

“If your company plays in a privacy-sensitive industry, your customer databases may be empty in a few years if you don't start investing in privacy now. If customers can't see the results of the investment, privacy won't pay.”

Computerworld, 2003

Why Post a Privacy Statement?

You may be required to post a privacy statement. In recent years, a number of privacy laws have been enacted, forcing many companies to play catch-up in the privacy arena or face steep fines and lawsuits.

Much of the current privacy legislation is industry-specific.

Privacy Legislation

Financial service companies must post a privacy statement outlining certain data security measures under the Gramm-Leach-Bliley Act (GLBA).

Children's sites must obtain verifiable parental consent before gathering information from children under the Children's Online Privacy Protection Act (COPPA).

Sites doing business with the European Union are subject to the EU Data Directive, regulating the collection, use and security of personal information regarding EU citizens.

Medical and insurance sites may be required to comply with the Health Insurance Portability and Accountability Act (HIPAA), regulating the collection, use and storage of health-sensitive information.

The newest privacy legislation has much broader implications.

Additionally, in October of 2003, California passed the Online Privacy Protection Act, reflecting the growing expectation for vigilance in the privacy arena. The Act gives companies only nine months to come into full compliance. By July 2004, every Web site either in California or collecting personal information from California consumers must post a privacy statement online.

The Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada now requires all Canadian industries and organizations to comply with its privacy rules.

Why Post a Privacy Statement?

Posting a privacy statement online is the industry standard. Most Web sites now post an online privacy statement. This trend is in response not only to growing consumer concerns, but also mounting sentiment within the industry that e-businesses were gaining the reputation of being irresponsible data handlers susceptible to hackers and other security breaches. In addition to allaying consumer anxieties, creating and maintaining a privacy policy forces a company to understand its data-handling practices and may reveal potential liabilities that could threaten and undermine its brand.

Creating a privacy statement can help a company expose internal weaknesses in its data management processes.

Creating a privacy policy requires a company to undergo a thorough evaluation of the ways in which it collects, processes, uses, shares, and stores consumer data. This involves taking a comprehensive look at privacy and security, reviewing everything from personnel responsibilities to service-provider contacts and from Web encryption to offline data storage. An organization must delve into the details of how personal information is handled and shared both internally and externally to identify potential weaknesses.

The need to create a privacy policy too often occasions a company's first assessment of its data-handling protocol and many companies are surprised to learn that their consumer data is not as well-protected--and its personnel policies not as well-defined--as they may have assumed. Of course, it is always better for a company to uncover any shortcomings on its own rather than having them exposed to the public.

“Privacy isn’t just a problem for consumer-oriented business. It affects all businesses, regardless of whether they deal with individual consumers or solely with other enterprises.”

Intelligent Enterprise, 2003

Who Creates a Privacy Statement?

Unless your company is extremely small, chances are good that more than one person will be involved in the creation of your internal privacy policy and, thereafter, your public privacy statement. Members of your management, legal, marketing, operations, and engineering teams may each play a role.

Creating a comprehensive privacy statement involves input from representatives of many areas in an organization.

Key Privacy Personnel

Management. The leaders of an organization determine the overall privacy structure and the direction to take.

Legal. Legal experts will ensure that the written policies reflect a company's actual practices.

Marketing. Marketing personnel keep track of a company's current and projected future use of consumer marketing data.

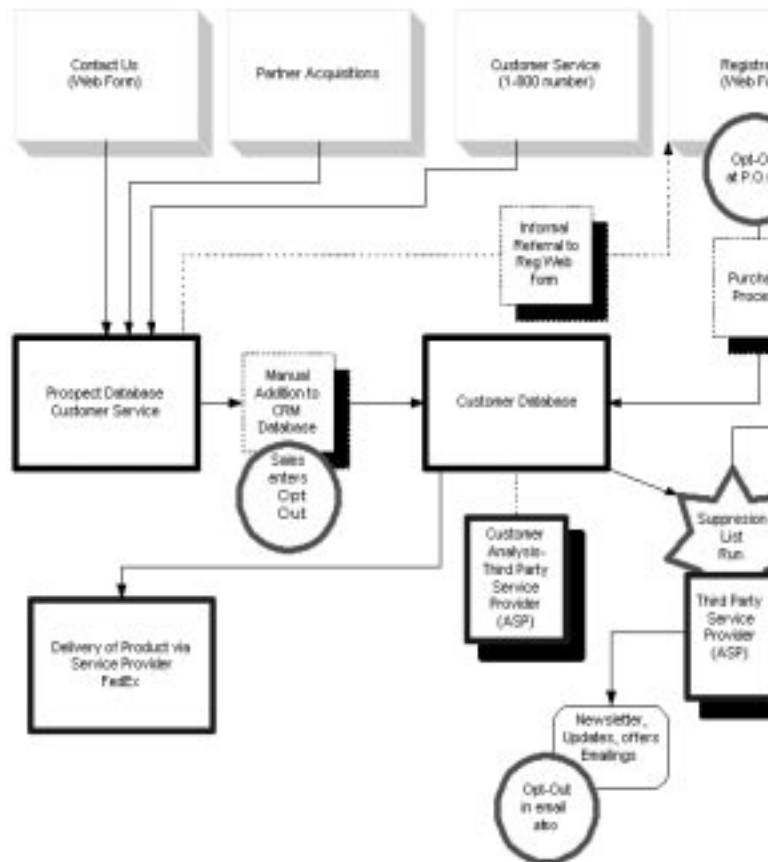
Operations. Those who oversee internal operations can map out and verify a company's workflow and data flow.

Engineering. Information architects know the detailed processes behind a company's transactions and databases.

Who Creates a Privacy Statement?

Sketching out a personal information flow chart is a good way to determine all points of consumer-company contact, to identify which employees come into contact with consumer data, how it is shared outside the company, how and where it is stored, and how it is archived or destroyed.

A data flowchart can help your organization understand your current data-handling practices and anticipate problems that could arise in the future.



This sample map shows the typical flow of data for a retail Web site. At the top level are the company's various collection points for customer data: Web forms, a customer service hotline, and partner acquisitions. The chart then goes on to show for what purposes customer information will be used, at which points a customer is allowed to exercise choices, and how these choices are incorporated into the data.

Who Creates a Privacy Statement?

Once there is a general understanding of how data flows through your organization, operations personnel can begin to dig deeper, usually by asking questions of the people involved at each level of the data map.

Questions should be directed to any employees that come into contact with consumer data, including the data engineers who maintain a company's information infrastructure, the communications personnel who seed the customer databases, and the marketing personnel who control use of the information stored in company databases.

Once you have a detailed understanding of how personal information is collected, maintained, and used within your organization, the legal or communications team can step in and draft your privacy statement. At this point the legal team can also make recommendations about how to improve data-handling practices if problems are uncovered during the assessment period.

It's extremely important that all the relevant parts of your organization have an opportunity to address privacy issues during the process of creating the privacy policy. If relevant players are left out, not only will the policy be incomplete, it could also end up short of an accurate picture and land your company in legal hot water.

“Privacy requires an integrated approach from both policy and technical perspectives...as a corporate cultural issue, privacy cuts across diverse areas of technology, organization, and regulation.”

Cisco Systems, 2002

What does a Privacy Statement Cover?

At a minimum, a privacy statement should cover the five elements of the Fair Information Practices. This section outlines what types of disclosures are covered under each of the five elements. For best practices, see the following expanded section, “What are Consumer-Friendly Privacy Practices?”

Clear notice forms the basis of any privacy statement.

Notice.

What information is collected. It may seem obvious that consumers would have full knowledge of what information is collected from them, but this isn't always the case. There are two types of information collection: active and passive. Active collection is the obvious form and involves information that users enter about themselves into Web forms. Usually, this information is for contact (like a name and address), financial (a credit card number), or identification (a password) purposes. There is also information that sites can passively collect without users actually having to enter anything. Passive information collection usually involves the use of tracking technology (like cookies or single-pixel GIFs) that harvests information like IP addresses or surfing behavior.

How information is used. Disclosure of how information is used is as important as what information is collected. In a privacy statement, a Web site should disclose how customer information will be used, including marketing purposes (like cross-selling, list-sharing, joint use), data to third parties, or combining customer data with other data for market research or other purposes.

Choice.

Web sites should provide users with choice regarding the dissemination and use of their personal information and should inform users of the choices available to them. Choice is typically presented in two ways: ‘opt-in’ and ‘opt-out.’

Legislators and consumer groups are pushing for expanded levels of choice.

Opt-in mechanisms require users to actively give consent, usually by checking boxes or clicking buttons to signify that they would like to have information shared in a certain way. Opt-out mechanisms, on the other hand, make consent the default setting, and users must actively un-check boxes or click out of certain modes to avoid having information shared.

While some Web sites will automatically include consumers on all of their mailing lists, giving consumers broader ranges of choice establishes and increases trust with Web sites.

What does a Privacy Statement Cover?

Access.

Web sites should allow users access to update or correct information they have provided online. If direct consumer access cannot be granted, sites should provide a way for users to request that information be corrected or updated.

Security.

Web sites should take security precautions to ensure data integrity. Industry standard is to encrypt all pages asking for Social Security Numbers or credit card data with Secured Socket Layers (SSLs). Most browsers will notify consumers when they are on secured pages.

Redress.

Web sites should have a formal process for managing and addressing consumer concerns. At the very least, contact information must be displayed, so consumers can contact the appropriate employees should privacy issues arise.

What are Consumer-Friendly Privacy Practices?

The most privacy-conscious companies set rigorous standards for themselves in protecting the privacy of their consumers. This section outlines some of the industry's best practices.

Minimize the amount of data collected.

Notice.

What information is collected. Although there are many marketing and research benefits to storing robust databases of consumer information, the less information a company collects, the easier it is to limit disclosures, minimize liability, increase security, and establish trust. While consumers may readily disclose whatever information is required to complete their online transactions, they become suspicious of sites that ask for extraneous information.

How information is used. Consumer information should not be used for purposes other than what it was obviously intended. For example, if a mailing address is provided for shipment of a product, the same mailing address should not be used to populate lists for catalogs or solicitations, even if they come from the original company that collected the address. The exception to this standard is if a legal procedure requires the disclosure of consumer information. A disclaimer to this extent, however, should certainly be made public in a privacy statement.

Provide clear choices for users.

Choice.

Industry surveys show consumers prefer opt-in consent modes for uses of their personal information. Nowadays, more consumers are demanding 'double opt-in' mechanisms to signal consent—usually active check-boxes with a follow-up email or pop-up asking if users are certain that they want to share information in a certain way. Particularly in email, acting responsibly can mean the difference in higher response rates and increased trust.

Left, an example of an opt-in mode of consent. Users must check the bottom box in order to receive a newsletter.



Right, an example of an opt-out mode of consent. Users must fill the 'No' radio button to avoid receiving an email.



What are Consumer-Friendly Privacy Practices?

Allow users easy access to their information.

Access.

It is required to allow users access to the information they provided with entry of a secure password or other comparable means of identification.

Comprehensive measures should be taken to ensure consumer privacy.

Security.

In addition to encryption of pages collecting sensitive information, the most comprehensive online practices also take into consideration other elements of data security, including personnel access to company databases, and offline data storage. Sites should employ authentication procedures (such as a password) when allowing users access to information they have provided. When making disclosures about security procedures, companies should take care not to disclose too much information to avoid breaches of security.

Consumers should have a third-party avenue to address privacy-related concerns.

Redress.

Sites should provide contact information for consumers to communicate their privacy-related concerns. Although email may provide the most efficient means of cataloguing problems, consumers also appreciate when live assistance is available.

Industry best practice is to additionally employ a third-party dispute resolution system to ensure consumers that fair decisions are made and enforced. It's important to many consumers to have an unbiased, outside party weigh both sides of an issue before deciding what course of action should be taken.

Consumer-Friendly Privacy Statements

Statements should be comprehensive and go into appropriate detail.

Consumer-friendly statements are thorough. TRUSTe requires its members to post disclosures of

- (1) What personally identifiable information is collected
- (2) What personally identifiable information third parties collect through the Web site
- (3) What organization collects the information
- (4) How the organization uses the information
- (5) With whom the organization may share user information
- (6) What choices are available to users regarding collection, use and distribution of the information
- (7) What measures the organization takes to protect the information under its control

For a good example, see www.basspro.com. Basspro does a great job of going through all of these topics and telling consumers, in plain language, how their personal information is used to process orders and who may have access to their information.

Additionally, a thorough privacy statement should cover privacy practices offline as well as online, if those practices pertain to information collected online. For example, if a company uses a shipping company to deliver consumer products, the relationship with the service provider should be disclosed in the privacy statement.

Statements should be easily accessible.

Consumer-friendly statements are accessible. A solid statement isn't worth much if consumers can't easily locate it. Statements should be displayed prominently, especially around areas where consumers are encouraged to share personal information. 1-800-DENTIST makes sure that its privacy statement is accessible directly beneath its form on the home page collecting personal information.

The average consumer should be able to understand the privacy statement.

Consumer-friendly statements are easy to understand. Statements can be clear without resorting to 'legalese.' Dynadirect clearly explains what SSL-encryption is and shows an image of a navigation bar explaining to consumers how to tell when they are on an encrypted page.

Statements should be of reasonable length.

Consumer-friendly statements are neither too short nor too long. Consumers are turned off by lengthy privacy statements but also want to be assured that a site addresses all pertinent topics. Many sites cleverly deal with this challenge by giving consumers the option of reading both short summaries and longer, more detailed explanations. eHealth gives short, bolded summa-

Consumer-Friendly Privacy Statements

ries of each of its policies, followed by longer explanations that make it easy for consumers to skim as well as explore the company's privacy policies. It also lists additional privacy topics at the bottom of the statement. Some sites, like Bolt, shorten their statement by linking to the longer explanations on an entirely separate page.

Statements should be prioritized for consumer relevance.

Consumer-friendly statements are prioritized. Because statements are consumer-facing, they should list the most relevant information first.

Consumer-friendly statements are updated as needed. Corex clearly signals to its consumers when it has updated its privacy statement. A stagnant statement may indicate to consumers that a company does not regularly review its privacy policies.

Privacy Resources

Privacy Exchange

<http://www.privacyexchange.org/>

PrivacyExchange compiles a bi-weekly e-newsletter, the PrivacyExchange NewsFlash, full of new and developing issues in privacy.

Privacy & American Business

<http://www.pandab.org>

Privacy & American Business researches privacy issues from a business standpoint.

The International Association of Privacy Professionals

<http://www.privacyassociation.org>

The International Association of Privacy Professionals is a network of privacy officers from different industries around the world.

EPIC

<http://www.epic.org>

The Electronic Privacy Information Center posts legislative and technological updates from the realm of privacy.

TRUSTe

<http://www.truste.org>

TRUSTe administers a Web privacy seal program and publishes a monthly e-newsletter containing privacy event listings, expert discussions on current legislation, and technical tips to keep companies and Web sites up to date.

Sources

1. Westin, Alan F. "Consumer Privacy Attitudes: A Major Shift since 2000 and Why." *Privacy & American Business Newsletter*: September 2003, v. 10, no. 6.
2. According to an August 2003 BizRate.com consumer survey. These figures were consistent with a similar survey conducted in January 2003.

Cisco Systems: "Privacy and the Law." 1999-2002.

Cline, Jay. "Does Privacy Pay?" *Computerworld*: June 17, 2003.

Fogg, B.J.; Kameda, T.; Boyd, J; Marshall, J.; Sethi, R.; Sockol, M.; and Trowbridge, T. (2002). "Stanford-Makovsky Web Credibility Study 2002: Investigating what makes Web Sites Credible Today." A Research Report by the Stanford Persuasive Technology Lab and Makovsky & Company. Stanford University. Available at www.webcredibility.org.

Madsen, Mark. "Making Your Privacy Policy Work." *Intelligent Enterprise*: June 28, 2002.

Peppers & Rogers Group "Privacy: Beyond Compliance. Responsible Information Stewardship." 2003.

Ponemon, Larry. "Turning Privacy Cost into Privacy Value." *Privacy Strategies for Customer-Centric Business*. Peppers & Rogers Group: 2002.