

# 3: WEB PRIVACY PRINCIPLES

The way people feel about sharing personal information—especially computerized information—can vary significantly, between countries, between companies, and between individuals. However, some general principles have evolved over the years and have been widely accepted in many quarters. The goal of this chapter is to review these principles and understand their importance to businesses, particularly those that have Web operations.

## ***Basic Privacy Principles***

Why do you need to be aware of basic privacy principles? The main reason is that a lot of privacy law in the United States today is based upon them. You can see these basic privacy principles at work in laws which impose specific legal requirements on Web sites, such as the Children’s Online Privacy Protection Act (COPPA: 1998) and the Health Insurance Portability and Accountability Act (HIPAA: 1996). These laws are described in more detail in Chapter 4. Basic privacy principles have also shaped older laws such as the Fair Credit Reporting Act (FCRA: 1970), as well as legal actions and regulatory decisions regarding privacy, such as those by the FTC against Eli Lilly, Doubleclick, and Microsoft.

The second reason for knowing about these principles is that they have guided the privacy legislation of many countries outside the U.S. In fact, some countries have elevated basic privacy principles to the level of privacy *rights*, which means that in many cases, personal data enjoys legal protection by default. This is not the case in the U.S., which has taken a piecemeal approach to privacy legislation. For example, there are more than 30 federal laws that address data privacy topics as specific as video rental records,

school records, and the use of driver's license data. Thus, some personal data are protected by federal laws, others are not. At the same time a complex patchwork of privacy laws exists at the state level—also drawing on basic privacy principles—and there is a growing body of privacy case law arising from legal actions brought by individuals and regulators.

More privacy laws will probably be enacted at the federal level in the next few years, and they will tend to mirror basic privacy principles. Certainly more American companies are engaging in international business via the Web. So another reason for acquainting oneself with these privacy principles is their ability to provide a default approach to privacy that will meet standards for best practices well into the future, and just about anywhere your business takes you. A good example of this is Apple Computer, which has committed itself to a "highest common denominator" approach to privacy, intending to meet international privacy standards even when they are higher than domestic requirements.

## **Early U.S. Laws**

The first major federal legislation to reflect basic privacy principles was perhaps the Freedom of Information Act, or FOIA, enacted in 1966. The FOIA established the general principle that any person has a right of access to federal agency records. The FOIA provides access to all federal records (or portions of those records) except those protected from release by nine specific exemptions:

1. classified national defense and foreign relations information,
2. internal agency personnel rules and practices,
3. material prohibited from disclosure by another law,
4. trade secrets and other confidential business information,
5. certain inter-agency or intra-agency communications,
6. personnel, medical, and other files involving personal privacy,
7. certain records compiled for law enforcement purposes,
8. matters relating to the supervision of financial institutions, and
9. geological information on oil wells.

The FOIA does not apply to Congress or the courts, nor does it apply to records of state or local governments. However, nearly all state governments have their own FOIA-type statutes. The FOIA does not require a private organization or business to release any information directly to the public, whether it has been submitted to the government or not. However, information submitted by private firms to the federal government may be available through a FOIA request provided that the information is not a trade secret, confidential business information, or protected by some other exemption.

Closely related to the Freedom of Information Act is the Privacy Act, another federal law regarding federal government records. The Privacy Act, the emergence of which will be discussed in a moment, establishes certain controls over how the executive branch agencies of the federal government gather, maintain, and disseminate personal information (like the FOIA, the Privacy Act can also be used to obtain access to information, but it pertains only to records the federal government keeps on individual citizens and lawfully admitted resident aliens; the FOIA covers all records under the custody and control of federal executive branch agencies).

The Fair Credit Reporting Act of 1970 was probably the first federal legislation in the United States to refer to “the consumer’s right to privacy.” However, this law is very narrowly focused and does not specifically address computer-based information. The FCRA, which was substantially overhauled in 1996 by the Consumer Credit Reporting Reform Act (CCRRA) had a very narrow intent: to protect consumers from the disclosure of inaccurate and arbitrary personal information held by consumer reporting agencies. Although the FCRA regulated the disclosure of personal information, it did not restrict the amount or type of information that could be collected.

## ***The Hew Report***

You might be surprised to learn that the first U.S. legislation to consider privacy specifically in the context of computers appeared in the early seventies. Elliot Richardson, who was Richard Nixon’s Secretary for Health, Education and Welfare, commissioned a study of record-keeping practices in the computer age. The resulting report, commonly known as the “HEW Report,” recommended the

enactment of a federal “Code of Fair Information Practice” for all automated personal data systems. The code envisioned by HEW contained five principles that would be given legal effect as “safeguard requirements” for automated personal data systems:

1. There must be no personal data record keeping systems whose existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him that was obtained for one purpose being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

While it is unlikely to impact business Web sites directly, the Privacy Act of 1974 is worth knowing about because it embodied the HEW principles in law, establishing protections for personal data held by the federal government. And although the law only applies to the federal government, it is important to note that the federal government compiles a wide range of information on individuals. For example, if you were ever in the military or employed by a federal agency, there should be records of your service. If you have ever applied for a federal grant or received a student loan guaranteed by the government, you are probably the subject of a file. There are records on every individual who has ever paid income taxes or received a check from Social Security or Medicare.

The Privacy Act establishes certain controls over what personal information is collected by the federal government and how it is used. The Act guarantees three primary rights:

1. the right to see records about yourself, subject to the Privacy Act’s exemptions,
2. the right to amend that record if it is inaccurate, irrelevant, untimely, or incomplete, and

3. the right to sue the government for violations of the statute including permitting others to see your records unless specifically permitted by the Act.

The Privacy Act also provides for certain limitations on agency information practices, such as requiring that information about a person be collected directly from that person to the greatest extent practicable; requiring agencies to ensure that their records are relevant, accurate, timely, and complete. ; It also prohibits agencies from maintaining information describing how an individual exercises his or her First Amendment rights unless the individual consents to it, a statute permits it, or it is within the scope of an authorized law enforcement investigation (note that this description of the Privacy Act, and some of the preceding documentation of the FOIA, are taken from public domain documents published by the federal government).

## **The OECD Guidelines**

Another important set of data privacy principles was published in 1980 by the Organization for Economic Cooperation and Development. The OECD is comprised of thirty countries bound together by three principles: pluralistic democracy, respect for human rights, and open market economies. The OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" were adopted by the organization in 1980 in support of these principles. The full text of the document, which is often referred to simply as "the OECD Guidelines," can be read online at the OECD web site ([www.oecd.org](http://www.oecd.org)). You can also buy a hard copy or license a printable electronic version. The following is a summary of the privacy principles the document sets forth:

- **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

- **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in the Purpose Specification Principle, except with the consent of the data subject or by the authority of law.
- **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the Data Controller.
- **Individual Participation Principle:** An individual should have the right:
  - a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
  - b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
  - c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
  - d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- **Accountability Principle:** A Data Controller should be accountable for complying with measures that give effect to the principles stated above.

These principles have guided the development of privacy laws in many countries, including Canada, Australia, Singapore, Hong Kong, and the fifteen member countries of the European Union (EU). For example, you can see them reflected in the U.K. Data Protection Act of 1998, which includes a statement of eight enforceable principles of good practice with which anyone processing personal data must comply. These state that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

---

**1984!** The first U.K. Data Protection Act was passed in 1984. By the time it was revised in 1998, personal data was being defined very broadly, to include “both facts and opinions about the individual” and “information regarding the intentions of the data controller towards the individual.” The definition of processing was also widened and now incorporates the concepts of ‘obtaining’, ‘holding’ and ‘disclosing’

---

As you can see there are many similarities between the OECD and U.K. principles and those in the HEW Report. However, you may have noticed several terms that are not in the HEW principles: data subject, data controller, and transborder data flows. Each of these will be explained in turn, starting with data subject, which, as we noted in Chapter 1, is simply a handy way of saying “the individual described or identified by the data.”

## Data Controller

The term data controller is more complex and refers to a concept that is widely used in Europe but less so in the United States. Here is how data controller is defined in Britain's Data Protection Act:

“a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.”

In Europe the concept of a data controller is seen as essential to the implementation of basic privacy principles such as those in the HEW Report, namely:

- finding out what information about yourself is in a record,
- preventing information about yourself that was obtained for one purpose from being used or made available for other purposes without your consent,
- correcting or amending a record of identifiable information about yourself.

In other words, unless there is a way to identify persons in control of personal data, it is very hard to protect the privacy of the persons described by the data, the data subjects. Thus the accountability principle specifically refers to the role of the data controller. The British law stresses the importance of establishing whether or not someone is a data controller, because it is data controllers who are required to comply with the data protection principles. Section 4 of the Act states:

“it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.”

Under privacy protection laws in Britain, and many other European countries, a data controller is a “person” in the legal sense, a term which comprises not only individuals but also organizations such as companies and other corporate and unincorporated bodies of persons (for example, a homeowners’ association, a country club, a public company, or a sole proprietor). If your company does business in Europe it is almost certain to be a data controller.

## **Transborder Data Flows**

One of the main motives for the OECD to develop privacy guidelines was the need to encourage international harmonization of

---

privacy laws, without which the free flow of economically necessary personal information could be interrupted. In other words, more than two decades ago the OECD anticipated that cultural and political differences between Members—the countries that make up the OECD refer to themselves as Members—could result in differing standards for data protection, which might create a reluctance to allow personal data to cross borders, thereby impeding business.

---

**No Flow:** There are several examples of differing standards for data protection resulting in reluctance to allow personal data to cross borders. In 1991 an airline operating under Swedish law was not allowed to deliver personal data to U.S. Customs without first warning passengers of the inadequacies of U.S. data-protection laws, and therefore obtaining informed consent. In another case, a German data processing bureau was prevented from carrying out its processing in the United Kingdom, due to inadequacies in U.K. law. France even required contractual guarantees of adherence to French law before Mormon genealogical records could be transferred to Utah.

---

As the OECD Guidelines state: “although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information.” The Guidelines also note “automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices.” Since the flow of personal data across borders contributes to economic and social development it would be undesirable for “domestic legislation concerning privacy protection and transborder flows of personal data” to hinder such flows. The Guidelines thus recommend that Member countries:

1. take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties (that is, the ones summarized above);
2. endeavor to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
3. co-operate in the implementation of the Guidelines;
4. agree as soon as possible on specific procedures of consultation

and co-operation for the application of these Guidelines.

In 1985 the OECD followed through on item four by publishing the "Declaration on Transborder Data Flows." This was further evidence of the desire of Member countries to affirm the general spirit in which they would address these issues. The Declaration began by acknowledging that computerized data and information were now circulating freely on an international scale and significant progress had been achieved in the area of privacy protection at national and international levels. It then stated the four things Member countries would do to further their goals:

1. *Promote* access to data and information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information;
2. *Seek* transparency in regulations and policies relating to information, computer and communications services affecting transborder data flows;
3. *Develop* common approaches for dealing with issues related to transborder data flows and, when appropriate, develop harmonized solutions;
4. *Consider* possible implications for other countries when dealing with issues related to transborder data flows.

This might sound like very abstract, high-level stuff, but it does have practical implications for Web site privacy, especially if you operate multiple Web sites in different countries, or even one site in one country that processes personal data from multiple countries. Chapter 5 will address the practical implications of transborder personal data flows, including several means by which companies can avoid some of the problems that can arise when such data needs to flow into the United States. The point to note here is that the privacy principles at work internationally were established some time ago and at a very high level.

## ***Fair Information Practice Principles***

So, basic data privacy principles were being discussed long before the commercialization of the Internet. In 1998, the U.S. Federal Trade Commission reiterated these principles in the context of the

Internet when it produced, at the request of the legislative branch, a document called “Privacy Online: A Report to Congress.” The report began by observing that:

“Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information—their “information practices”—and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.”

Since its publication, this report has helped to shape the current “privacy-enforcement” role of the FTC. This role, about which every Web site operator needs to know, is discussed in Chapters 2 and 6. In this chapter, we focus on the five core principles of privacy protection that the FTC determined were “widely-accepted,” namely: Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, and Enforcement/Redress. Each will be described in turn, together with some practical implications.

## Notice/Awareness

*Notice* is a concept that should be familiar to network professionals. Many systems, including many Web sites, put users on notice with respect to ownership, security, and terms of use. Such notice might be a banner that appears during network log-on, warning that access to the network is restricted to authorized users. It might be a splash page for a Web site informing visitors that clicking to enter constitutes agreement to the terms of use. In the context of Web site privacy, notice means you must advise visitors to your site of your policies with respect to the personal data you process. As the FTC puts it:

“Consumers should be given notice of an entity’s information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles (choice/consent, access/participation, and enforcement/redress) are only meaningful when a consumer

has notice of an entity's policies, and his or her rights with respect thereto."

In practical terms, the primary means of providing privacy notice to Web site visitors is the privacy statement, described in Chapter 1 and discussed in detail in Chapter 6. For simple sites that set no cookies or receive no user input, such a statement is easy to draft. The more complex and interactive the site, the more work it will take to craft a statement that covers all the bases. Here are the main points that need to be covered:

- Identification of the entity collecting the data.
- Identification of the intended use of the data.
- Identification of any potential recipients of the data.
- The nature of the data collected and the means by which it is collected, if not obvious (for example, passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information).
- Whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information.
- The steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data.

Of course, it might not be your job to pull together this information and come up with a privacy statement—in recent years, many large organizations have been appointing chief privacy officers to oversee the creation of privacy policies for the organization and its Web sites. Nevertheless, if you are responsible for the Web site, you may be asked to do some of the work, notably documenting logging activity and the use of cookies. The following sections briefly discuss these issues and they are addressed again—in the context of writing privacy statements—in Chapter 6.

**Logging Activity:** You need to let visitors to your site know if you use automated tools to log information about their visits (information such as the type of browser and operating system they used to access your site, the date and time they accessed the site, the pages they viewed, and the paths that they took through the site).

**Use of Web Bugs and Beacons:** Use of these techniques should be disclosed, along with a clear statement of how and why they are used, and what information they track. (for more on this topic, see Chapter 6 and the Sources section at the end of the book).

**Use of Cookies:** Use of cookies should be disclosed and a distinction should be made between *session* cookies, which expire when the user closes the Web browser, and *persistent* cookies, which are downloaded to the user's machine for future use on the site.

## Choice/Consent

Like Notice/Awareness, this second principle should be addressed with honesty and sensitivity. *Choice* means giving consumers options as to how any personal information collected from them may be used. This relates to secondary uses of information, which the FTC describes as “uses beyond those necessary to complete the contemplated transaction.” The FTC notes that “such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.”

Whether or not you are involved in deciding what use is made of personal information that comes from your Web site, you need to know whether you are going to give users of the site any choice in the matter, even if it is something as simple as a check box that says “You may e-mail me about special offers on related products.” As you might expect, privacy advocates prefer the opt-in form of consent, in which people specifically request to be included on a mailing list, rather than opt-out, which adds people to the list by default, until such time as they request to be removed (there is more on these terms in the section “Options for Opting,” later in the chapter).

## Access/Participation

The point of *access* and *participation* is to let people about whom you have information find out what that information is, and contest its accuracy and completeness if they believe it is wrong. Many online systems currently lack the means to implement such processes

securely. However, access is considered an essential element of fair information practices and privacy protection. In the context of business Web sites, the main obstacle to providing access and participation is a lack of cheap and secure methods of reliably identifying, that is, authenticating, the data subjects.

Compliance with U.S. laws that mandate access, such as the Fair Credit Reporting Act, is accomplished right now through more traditional channels of communication, such as letters and faxes. Both require human participation and review. Unless you have a high level of assurance that you are giving online access to the appropriate person—such as multiple factor authentication—there is a serious risk that providing access in support of privacy will actually lead to privacy breaches (for example, through unauthorized disclosure to someone posing as the data subject).

---

**Watch Out:** More and more companies are finding that the cost of communicating with customers via the Web and e-mail is much lower than communicating via voice or paper. Consequently, management will want to explore, sooner or later, data subject access to company PII databases through the Web site and/or e-mail. Unfortunately, until the security of the underlying technology improves, this strategy is fraught with risks, such as unauthorized disclosure through spoofing, pretexting, or the interception of unencrypted e-mail. Do not attempt unless management is fully aware of the risks and prepared to fund appropriate levels of additional security.

---

## **Integrity/Security**

The fourth widely accepted principle is that data be *accurate* and *secure*. To assure data *integrity*, data collectors, like Web sites, must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form. Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include the following:

- Limiting access through access control lists (ACLs), network passwords, database security, and other methods
- Storing data on secure servers that cannot be accessed via the Internet or modem
- Encryption of data during transmission and storage (Secure Sockets Layer, or SSL, is considered acceptable when submitting information via a Web site—but note that, unless the client system has a digital certificate or other authentication upon which the server can rely, SSL may not be acceptable for disclosure from server to client).

## Enforcement/Redress

The FTC has observed that “the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.” What that mechanism is for your Web site will depend on several factors. As you will see in the next chapter, your Web site may have to comply with specific privacy laws. Your organization may subscribe to an industry code of practice or *privacy seal program*, both of which may include dispute resolution mechanisms and consequences for failure to comply with program requirements. A private action against your organization is also a possibility if the organization is found to be responsible for a breach of privacy that caused harm to an individual. Class-action lawsuits have also been brought, alleging privacy invasion. In Chapter 9, the general oversight role of the government will be discussed; specifically the willingness of the FTC to find that failure to live up to privacy policies constitutes deceptive business practice.

## Options for Opting

Before concluding this chapter and our review of privacy principles, some practical consideration must be given to the principle of choice and the terms “opt-in” and “opt-out.” Visitors to a commercial Web site typically make a number of choices about the use and disclosure of their personal information. For example, the site may allow visitors to make purchases. Visitors supply their name and other information necessary to complete a purchase transaction, typically via a user input form. Reference has already been made to

the value of reinforcing general privacy notices with specific notices on forms. For example, a product order form might state that information submitted via the form will be used to complete the order and nothing more.

Of course, if a visitor to your Web site has gone so far as to start filling out an order form, you may want to make the most of the opportunity. For example, in the offline world it is standard practice to mail catalogues and product news to people who have purchased from you. Some people appreciate this, others object, usually by requesting that you stop sending mail to them. In other words, the customer has a choice to *opt-out* of your mailing list.

Things work a little differently online, mainly because people perceive email to be quite different from postal mail (see Advice column). So, to continue our example of Web site visitors who are interested in purchasing your products or services, you may want to think twice before assuming that this interest equates to permission to send them email that is not directly related to that purchase. What you can do, entirely in keeping with basic privacy principles, is give people a choice. You can include on the purchase form a suitable check box, labeled "Keep me informed of new products," or whatever choice it is you wish to offer, whatever permission you would like to have.

---

**Email Costs!** Whereas postal mail is paid for entirely by the sender, email is paid for, at least in part, by the people who receive it (through fees to the recipient's Internet Service Provider). Also, weeding out unwanted email is considered by many people to be more of a chore than ditching unwanted postal mail. Most Americans get one postal delivery per day per household. Compare that to the number of times per day the average email user gets a fresh batch of email delivered to his or her in-basket. Sorting out the unwanted email is not a once-a-day chore you can delegate, but a constant, personal distraction; hence the sensitivity that many people have developed to getting email they don't want.

---

The next consideration is whether or not the box is checked by default. Presenting the form with an unchecked box requires persons using the form to positively affirm their decision; in other words they *opt-in*. From a privacy perspective, this is the preferred approach to building mailing lists, particularly emailing lists.

---

Pre-checking a permission check box is generally frowned upon as presumptuous. Privacy advocates would argue that is the same as opt-out, that is, the person's permission is assumed, and their choice made for them rather than by them.

Some privacy advocates would like to go further and require what is known as *confirmed opt-in* or *double opt-in*. In this example, conformed opt-in means that when someone checks the box and gives permission to be contacted, the company then confirms this—for example, send the person an e-mail saying “You indicated that we may e-mail you about special offers on related products—please confirm this by replying to this message.”

While confirmed opt-in might seem like overkill, and may result in fewer names being added to your list—if there is no confirming email, the address cannot be added—there are some practical benefits. If you have ever worked with an opt-in list that did not require confirmation, you will know that a surprising number of people make mistakes when typing their e-mail addresses (which is why some forms require you to enter your email address twice). If someone who wants information from you enters her email address incorrectly, you both loose. She doesn't get the information she presumably wanted and, unless you have some other means of contact such as telephone or postal mail, you have no way of asking her to correct her email address. The confirmed opt-in method assures you that you are using a valid e-mail address for that person and you have their choice well and truly documented.

---

**Addressing Email :** There are several ways of improving your chances of getting a good email address when you ask for one. You can use a duplicate email address field and make sure the user types the same address twice. Unfortunately, some people simply do not know their email address (some think it is the alias that appears in an Outlook header, such as “Cobb, Stephen”). So you may want to validate the user input to make sure it fits these parameters: at least one allowable character preceding the @ character, followed by at least one allowable character and a dot, ending in a legal domain name (the definition of legal domain name in programming logic is a complex task, since there can be subdomains, but working back from the end on an address is one way to determine where an address is from, geographically speaking, which can be useful).

---

Marketers have tended to favor the *opt-out* approach to choice, which has several levels, the most basic being to use a person's information without any permission, until such time as he or she objects. (You may have encountered this approach in an e-mail message from a company you have never heard of, and it includes a link to opt-out from future mailings.)

To follow the example above, collecting information on your Web site, opt-out can mean several things. You can comply with the principle of *notice* by simply stating that any email address supplied may be used for marketing purposes, but this does not meet the *choice* requirement. Choice could be a box labeled "You may not contact me about special offers on related products." There is nothing to stop you leaving this unchecked by default. So the person filling out the form must specifically request that his or her information not be used. This will not please privacy advocates, but it is perhaps more honest than *pseudo-opt-in*, where "Yes" is pre-selected as the choice next to a "Use my data" check box (a practice that is particularly annoying to privacy-sensitive individuals).

The subtleties of opt-in and opt-out as they apply to emailing lists are addressed in more detail in the context of Web site privacy in Chapter 10. It is now time to look at how privacy principles have been implemented in privacy laws, which is covered in the next chapter.

# CHAPTER FOUR

# PRIVACY LAWS

0101011011100110111110100101110010101011011011



“I believe that the definite establishment of this right of privacy is at this time of the greatest possible moment; for, without such a right and the easy enforcement of it, civilization must deteriorate, and modesty and refinement be crushed by brutality and vulgar indecency.”

—John Gilmer Speed, “The Right of Privacy,” *The North American Review*, Volume 163, Issue 476, July 1896.