

Web Site Privacy Laws

This article sets out a general discussion of legal issues relevant to web sites of companies based in the United States.¹

1. Introduction
2. Section 5 of the U.S. FTC Act and Company Privacy Policies
3. Children's Online Privacy Protection Act
4. Gramm-Leach-Bliley Act
5. Health Insurance Portability and Accountability Act of 1996
6. European Union Data Protection Directive
7. The E. U. / U.S. Safe Harbor Principles
8. Some General Guidelines

1. Introduction.

A variety of laws and customs affect the capture, retention, use, sale or dissemination of information about persons accessing a Web site. In the United States, there is no single law or set of rules with universal application in this area. The U.S. federal government has encouraged industry efforts to develop self-regulatory regimes to ensure privacy online,² and the overall U.S. legal framework includes a mix of legislation, administrative action, and self-regulation. It has become common for Web sites to post a Privacy Statement disclosing what information the site captures about visitors, and what use is made of that information, often with procedures by which a visitor may give the site operator instructions about how to treat that visitor's information.³ Such a privacy notice is legally required in some situations,⁴ and in other

¹ This is a general article, not legal advice to any particular person, and does not create an attorney-client relationship. If you have questions of a legal nature, you should consult your own attorney. The author of this article is a member of the California Bar, and is not licensed to practice elsewhere. The article discusses certain U.S. federal laws and certain European Union requirements. It is not intended to cover all privacy laws relevant to Web sites, and, among others, does not treat U.S. state laws nor the laws of individual European countries

² See National Telecommunications and Information Administration, Department of Commerce, "Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy; Federal Register, June 5, 1998.

³ Protecting Consumers' Privacy: 2002 and Beyond, Remarks of FTC Chairman Timothy J. Muris at The Privacy 2001 Conference, Cleveland, Ohio, October 4, 2001, footnotes 12 and 13 and accompanying text, posted at <http://www.ftc.gov/speeches/muris/privisp1002.htm>.

⁴ For example, under the federal Children's Online Privacy Protection Act, discussed in Section 3, or the Gramm-Leach-Bliley Act, discussed in Section 4.

situations may be used as a matter of custom, to inspire user confidence, or to qualify for certification by TRUSTe or the BBBOnline Privacy Seal program.⁵ Some privacy laws affecting Internet sites, such as the Gramm-Leach-Bliley Act discussed below, apply to consumer transactions rather than transactions between businesses, and therefore may not generally be of concern to web sites that attract only business users. This is not true, however, in every case. The European Union Data Protection Directive, also discussed below, applies to personal information, regardless of whether it is acquired in a consumer transaction, or in some other manner. The next four section of this Article will discuss the application to web site privacy issues of Section 5 of the U.S. FTC Act, the European Union Data Protection Directive, the E. U. / U.S. Safe Harbor Principles, and the U.S. Gramm-Leach-Bliley Act.

2. Section 5 of the FTC Act and Company Privacy Policies.

Failure to abide by commitments made in a published privacy policy constitutes an unfair or deceptive trade practice in violation of Section 5 of the U.S. Federal Trade Commission Act. A well-publicized enforcement action based on this principle involved Toysmart, an Internet retailer of children's toys. Toysmart's privacy notice posted at its Web site had represented to consumers that personal information would never be shared with third parties. When the company went into bankruptcy, it announced a sale of all of its assets to generate funds to pay creditors. The customer database was one of the company's assets that was put up for sale. In July 2000, the U.S. Federal Trade Commission filed a complaint against Toysmart, seeking to prevent the sale of confidential, personal customer information collected on the company Web site. The complaint alleged that Toysmart had violated Section 5 of the Federal Trade Commission Act⁶ by misrepresenting to consumers that personal information would never be shared with third parties, and then disclosing, selling, or offering that information for sale. The FTC and Toysmart agreed to a settlement under which the company's Web site assets would have been sold only to a business in the family commerce market that would serve as a successor-in-interest as to the uses of the customer information. TRUSTe, which had awarded a seal of approval to Toysmart for its promise to adhere to TRUSTe online privacy guidelines, opposed the proposed settlement with the FTC, as did 39 state attorneys general. Bankruptcy Judge Carol Kenner refused to approve the sale guidelines agreed to by the FTC and Toysmart. Ultimately, Toysmart agreed to destroy its customer database rather than sell it, in exchange for a \$50,000 payment from a subsidiary of Walt Disney, which owned 60% of Toysmart, with the approval of the Bankruptcy Court. Another failed online toy retailer, eToys, ran into a similar problem (In re eToys Inc., Bankr. D. Del, Nos. 01-00706 (MFW)-01-00709 (MFW), 4/16/01).⁷

⁵ TRUSTe and BBBOnline are Internet privacy organizations that review the privacy practices of business web sites and permit businesses that meet their standards to display a privacy seal, for an annual fee that slides based on revenues. See <http://www.truste.org/about/truste/index.html> and <http://www.bbbonline.com/privacy/>.

⁶ “. . . unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful. . .” 15 U.S.C. 45; *Federal Trade Commission v. Toysmart.com LLC*, (U.S. District Court D. Mass, Civ. Action No. 00-11341-RGS); <http://www.ftc.gov/opa/2000/07/toysmart.htm>; <http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm>; http://www.truste.org/news/padvisories/users_toysmart_objection.html.

⁷ See also *GeoCities*, FTC Dkt. No. C-3849 (consent order entered on Feb. 12, 1999, settling charges that Web site misrepresented the purposes for which it was collecting personal identifying information from children and adults) and *Eli Lilly & Co.*, FTC Dkt. No. 012-3214 (Jan. 18, 2002 consent order with Eli Lilly & Company to resolve allegations that Lilly violated the FTC Act by claiming that it employed measures appropriate under the

The lesson of the Toysmart case and similar cases is that noncompliance with a company's online statement of how it collects and discloses information amounts to an illegal unfair and deceptive practice. Hence it is important for a company periodically to review both its written privacy statement policy and the company's actual practices.⁸

3. Children's Online Privacy Protection Act.

Under the U.S. federal Children's Online Privacy Protection Act⁹, privacy statements are required for commercial Web sites directed to children under 13 years old or general audience sites that have actual knowledge that they are collecting information from a child. The Web site must provide notice of what information is collected from children, how the operator uses such information, and the operator's disclosure practices for the information.¹⁰

Sites also must obtain verifiable parental permission before collecting information from children. The site operator must provide a requesting parent a description of the specific types of personal information collected from the child, and the opportunity at any time to refuse to permit the operator's further use, maintenance or collection, of personal information from that child. Sites may not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity. The web site operator must maintain reasonable procedures to protect the confidentiality and security of personal information collected from children.¹¹

4. Gramm-Leach-Bliley Act.

The U.S. federal Gramm-Leach-Bliley Act prohibits a financial institution from disclosing any nonpublic personal information about a consumer, unless it has given the consumer a privacy notice describing its policies and practices regarding disclosure and protection of information about customers and former customers.¹² The Act is directed at "financial institutions." The FTC's application of that term is surprisingly broad, however,

circumstances to protect the confidentiality of personal information obtained from consumers who visited its Prozac.com Web site, when in fact it did not), http://www.ftc.gov/os/2002/03/budgetstmt.htm#N_5.

⁸ Another implication of these cases is that due diligence on a potential business acquisition target should include close review of its historical privacy statements, particularly if there is a desire to use any customer information or other information gathered at the target's Web site.

⁹ 15 U.S.C. 6501 – 6505; regulations at 16 C.F.R. Part 312.

¹⁰ 15 U.S.C. 6502(b)(1)(A)(i).

¹¹ 15 U.S.C. 6502(b)(1)(B).

¹² 15 U.S.C. 6801 et seq., Public Law 106-102. Section 502 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6802, prohibits a "financial institution" from disclosing to a nonaffiliated third party any nonpublic personal information of a "consumer," unless such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form, that such information may be disclosed to such third party, and gives an opportunity to opt out of such disclosure. Section 503 of the Act requires that at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a financial institution disclose its policies and practices with respect to collecting, disclosing and protecting nonpublic personal information of customers and former customers. FTC Resources re Gramm-Leach-Bliley are posted on the Web at <http://www.ftc.gov/privacy/glbact/index.html>.

picking up universities, for example, presumably because they make student loans. Under Section 509 (3) of the Gramm-Leach-Bliley Act (15 USC 6809), “financial institution” is defined as “any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956,” 12 U.S.C. 1843(k). These activities include (among other things) lending, trust activities, insuring, underwriting securities, and other activities closely related to banking. To the extent that a company allows purchases on credit, a question therefore arises as to whether it could be considered a “financial institution” for this purpose. However, the Gramm-Leach-Bliley privacy requirements apply only to financial institutions that provide financial products or services to “consumers.”¹³

5. Health Insurance Portability and Accountability Act of 1996.

Pursuant to the Health Insurance Portability and Accountability Act of 1996, the U.S. Department of Health and Human Services has promulgated its Final Rule regarding Standards for Privacy of Individually Identifiable Health Information (the “HIPAA Privacy Rule”).¹⁴ The HIPAA Privacy Rule requires covered entities to provide a notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.¹⁵ Generally speaking, “covered entities” under HIPAA include health care providers who transmit health information in electronic form in connection with certain transactions covered by the HIPAA law, as well as health plans and health care clearinghouses.

A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its HIPAA notice of privacy practices on the web site. Also, in the case of a covered health care provider that provides services to individuals over the Internet, the provider must deliver the required notice of privacy practices to the individual electronically in response to the individual's first request for service.¹⁶

A HIPAA notice of privacy practices must be written in plain language and contain the following statement: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO

¹³ See Section A of the Federal Trade Commission's “Frequently Asked Questions for the Privacy Regulation” (December 2001), <http://www.ftc.gov/privacy/glbact/glb-faq.htm#A>. The FTC states “You have consumers if you provide your financial products or services to individuals, not businesses, to be used primarily for their personal, family, or household purposes.” If a company's customer base is businesses rather than consumers, it should not be subject to the privacy provisions of the Act, even if its extension of credit to customers could be construed as a “financial service.” See also the Federal Trade Commission's Privacy Rule, 16 C.F.R. § 313.3(k)(1), under which you are not a financial institution unless you are *significantly engaged* in financial activities.

¹⁴ 45 CFR Parts 160 and 164.

¹⁵ 45 CFR 164.520(a)(1).

¹⁶ 45 CFR 164.520(c)(2); Department of Health and Human Services release promulgating the Final Privacy Rule, Federal Register: December 28, 2000 (Volume 65, Number 250), Page 82725, available online from <http://aspe.hhs.gov/admsimp/>.

THIS INFORMATION.” PLEASE REVIEW IT CAREFULLY.” The HIPAA Final Privacy Rule contains additional details about the required contents of the notice.¹⁷

6. European Union Data Protection Directive.

In 1995 the European Union adopted a directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹⁸ (hereafter referred to as the “Data Protection Directive”). The Data Protection Directive was intended to harmonize the different national laws on data protection of the EU member states. It is not directly binding on private parties, but instead is a directive to the EU member states to adopt laws with certain features, within three years after October 24, 1995, the date of the Directive’s promulgation.¹⁹ The Data Protection Directive has been implemented into national law by most member states of the European Union.²⁰

Article 1(1) of the Data Protection Directive states the basic object of the Directive: “In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.” Note that the sentence quoted above refers to “natural persons,” and, in general, the Directive applies to information about individuals, not about companies.²¹

The Data Protection Directive lays out certain broad principles related to the collection, storage and use of personal information. First, an entity that controls the purpose and means of

¹⁷ See 45 CFR 164.520(b).

¹⁸ “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.” Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31.

¹⁹ See Article 32 of the Data Protection Directive. For example, in the UK, the Data Protection Act (1998) implements the EU’s Data Protection Directive. The UK Data Protection Act establishes an Information Commissioner, and makes it a criminal offense to process personal data without prior notification to the Information Commissioner. Note also that Articles 22 and 23 of the EU Data Protection Directive require member states to create a private cause of action against the data controller for violation of rights established pursuant to the Directive.

²⁰ As of late 2002, only Ireland and Luxembourg had not implemented the Directive, and both were expected to do so soon.

²¹ See also Recital 24 to the Data Protection Directive, “Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive.” The EU later adopted “Directive 97/66/EC of December 15, 1997 of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector,” referred to as the “Telecommunications Directive.” Unlike the Data Protection Directive, the Telecommunications Directive protects not only the personal data of individuals (‘natural persons’) but also the interests of legal entities (‘legal persons’). The Telecommunications Directive supplements the Data Protection Directive and provides for security of telecommunications networks, confidentiality of communications via public telecommunications networks, limitations on use and maintenance of telecommunications traffic data, and regulation of caller ID services, call forwarding, telephone number directories and unsolicited telephone calls. The requirements of the Telecommunications Directive, however, are mostly binding only on providers of publicly available telecommunications systems or on direct marketers.

processing personal data, referred to in the Directive as a “controller,”²² must notify the person to whom the data relates, referred to as a “data subject,” of the purpose of collecting personal information, and then the information must not be used for other purposes.²³

Secondly, personal data may be collected and processed only for legitimate purposes. Under Article 7, an “unambiguous consent” of the data subject makes data processing legitimate. Article 7 also specifies other situations in which processing of personal data is legitimate, although the criteria are somewhat vague. Article 14 requires that data subjects have a right expressly to be offered the opportunity to object, on request and free of charge, to the processing of personal data for the purposes of direct marketing, or to the disclosure of personal data to third parties or its use on their behalf for the purposes of direct marketing. Article 14 also mandates that data subjects have a right to object on “legitimate grounds” to the processing of data relating to them, and where there is a justified objection, to terminate such data processing. Here again, the criteria are vague, except that the right to say no to direct marketing appears clear.

Thirdly, the Data Protection Directive gives individuals a right to find out what information about them is being maintained, and to require that such information be accurate and current.²⁴ Fourthly, the Data Protection Directive mandates that member states require controllers to maintain the security of personal data against loss, theft or unauthorized disclosure.²⁵ Finally, the Data Protection Directive requires creation of government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin.²⁶

²² Article 2, Definitions, of the Data Protection Directive, provides: “. . . (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; . . .”

²³ Article 6 of the Data Protection Directive provides: “1. Member States shall provide that personal data must be: . . . (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. . . . (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; . . . (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. . . . 2. It shall be for the controller to ensure that paragraph 1 is complied with.” Article 10 provides that member states must require the party collecting information to state to the data subject: “. . . the purposes of the processing for which the data are intended; . . . the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, [and] the existence of the right of access to and the right to rectify the data concerning him. . . .”

²⁴ Article 12 provides for a right of individuals to confirmation of whether data about them is being retained, for what purpose, and to whom it may be disclosed, as well as a right to correction of inaccurate data.

²⁵ Article 17 requires member states to require controllers to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network. If the controller hires an outside party to process data, it must also have a written contract with the outside party requiring similar precautions.

²⁶ See Articles 18 through 20 of the Data Protection Directive.

7. The E. U. / U.S. Safe Harbor Principles.

Article 25 of the Data Protection Directive requires the member states to prohibit the transfer of personal data to a third country unless the country in question ensures an adequate level of protection, with certain exceptions including where the consent of the data subject has been obtained. Because of the difference in approach between the European Data Protection Directive, which establishes a comprehensive legislative and administrative framework, and the U.S. approach to privacy protection, which relies on a combination of much narrower legislation and self-regulation, Article 25 caused some concern for companies operating in both the U.S. and the EU, that may have data flowing out of the EU. In order to diminish uncertainty about whether transfers of information from Europe to the United States comply with the Data Protection Directive, the U.S. Department of Commerce, in consultation with the European Commission, developed Safe Harbor Principles.²⁷ The European Commission issued an "adequacy determination" for the safe harbor arrangement in July of 2000. Organizations receiving personal data transfers from the EU and complying with the Principles are considered to meet the "adequacy" requirements of the European Union's Directive on Data Protection. Hence, by certifying that they follow the Safe Harbor Principles, U.S. companies can assure EU organizations that a transfer to them complies with the Directive. The Safe Harbor Principles therefore provide a way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws.

Decisions by organizations to qualify for the safe harbor are entirely voluntary. An organization may qualify for the safe harbor by joining a self-regulatory privacy program that adheres to the Safe Harbor Principles, such as BBBOonline or TRUSTe. Alternatively, an organization may qualify for the safe harbor by developing its own privacy policies, provided that these conform with the Safe Harbor Principles.

The Safe Harbor Principles can be summarized as follows. An organization must inform individuals about the purposes for which it collects information, potential disclosures, and the individual's choices for limiting use or disclosure. An organization must offer individuals the opportunity to opt out of uses or disclosures of their personal information. For sensitive information such as that pertaining to health, race, political opinions, beliefs, trade union status or sex life, an affirmative opt-in is required for any use or disclosure. To transfer information to an agent, an organization must first determine that the agent subscribes to the Safe Harbor Principles or equivalent standards. Organizations controlling personal information must take reasonable precautions to protect the security of the information. Personal information may only be used in a manner compatible with the purposes for which it has been collected, and organizations should take reasonable steps to ensure that data is accurate. Individuals must have access to personal information about them that an organization holds and be able to correct it.

The Safe Harbor Principles require that there be some compliance mechanism in place, including dispute resolution procedures with damage awards for affected individuals, and sanctions for non-compliance by organizations that have announced adherence to the Safe

²⁷The Safe Harbor Principles are posted on the Web at www.ita.doc.gov/ecom, and information about the Safe Harbor is available at the Export Portal of the U.S. Department of Commerce, <http://www.export.gov/safeharbor/>.

Harbor Principles. But the company adopting the Principles has some choice over the form of the compliance mechanism. It can subscribe to a private sector dispute resolution program, such as TRUSTe's EU Safe Harbor program (http://www.truste.org/programs/pub_harbor.html) or the BBBOnLine Privacy Dispute Resolution Program (<http://www.bbbonline.org/privacy/dr.asp>). Alternatively, it can commit to cooperate with data protection authorities located in the European Union. In addition, if a company represents that it complies with the European Union Privacy Safe Harbor Principles and then fails to do so, the FTC can challenge that conduct as an unfair or deceptive trade practice under Article 5 of the Federal Trade Commission Act.

The European Union Data Protection Directive, and the Safe Harbor Principles, are potentially relevant to a U.S. based company, then, to the extent that the U.S. company receives personal data from Europe that it will maintain or "process" in some fashion. This information could be provided to the U.S. by a subsidiary or an unrelated entity. While information collected via the Web could trigger the application of the EU Data Processing Directive, so could information collected otherwise. For example, if the human services department of a U.S.-based company with European operations receives and maintains personal information about employees of the company's subsidiaries in Europe, the European subsidiary should be confirming that U.S. parent company has subscribed to the Safe Harbor Principles or otherwise demonstrated "adequate protection" before relaying such information to the parent company.²⁸ For U.S. based multi-national corporations, therefore, a review should be conducted of information flows between the company's European operations and the U.S. to determine whether signing on to the Safe Harbor Principles is warranted.²⁹ For companies that receive personal data from a limited number of European sources, a potential alternative may be to enter into private contracts, incorporating privacy clauses that meet the Data Protection Directive standards, with those European Union-based data controllers that may transfer personal information to them. For a company that receives personal information from a limited number of sources, this may be a less expensive method of compliance than signing on to the Safe Harbor Principles.

²⁸One U.S., company which has subscribed to the Safe Harbor Principles lists the following types of personal information received from the EU in its declaration to the Commerce Department: Personal Information Received From the EU: Personal information is collected for the administration of personnel services and employment processes in the context of employment relationship. The specific activities with respect to personal information received from the EU might include, among other things: (i) evaluation of qualifications for an employment position; (ii) provision of employment benefits; (iii) administration and management of compensation, training, and possible future career growth; (iv) making good use of individual's skills, (v) communicating with employees or their emergency contacts in case of abnormal circumstances; (vi) administration of company's business including budgeting, manpower planning, and organizational design, and (vii) authentication of the individual's identity when gaining access to computer system applications.

²⁹One can check which companies have notified the U.S. Commerce Department that they subscribe to the Safe Harbor Principles on the Internet at <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>.

8. General Recommendations.

A. Privacy statements should be written in language that is clear and easily understood (not computer-ese), should be displayed prominently, and should be made available before the Web visitor is asked to provide any personal information.

B. Any time you request personally identifying information from a visitor to your web site, such as the visitor's name, email address, mailing address, phone number or fax number, provide a brief explanation of why the information is requested and how it may be used. If providing this information may result in someone contacting the visitor, give the visitor a choice about this via either opt-in or opt-out.

C. Regarding collection and use of information, follow the rule of thumb: "Say what you do and do what you say." Periodically poll inside the company regarding what data is being collected. This may change from time to time, without necessarily coming to the attention of the those responsible for the company's privacy policy, so some vigilance is required. Also, periodically monitor for new laws in this area, as there is constant activity.

D. If your company or affiliated companies do business in Europe or have significant business dealings with Europe, review whether personal data is being transferred from Europe to your company in the U.S. in a manner that would require either signing on to the EU Data Protection Directive Safe Harbor Principles or adopting contractual provisions safeguarding the information. Also consider applying for a TRUSTe or BBOnLine seal, thereby reassuring visitors to your Web pages about the treatment of their information.