

Subj: Online Privacy: Perspectives of Information Technology Association of America
From: Mark Uncapher, Vice President, ITAA, 703-284-5344, muncapher@itaa.org
To: Internet Caucus Advisory Committee

Excerpt From ITAA Online Privacy Statement: Internet Regulation & Digital Opportunity

Existing regulation

Beyond the restraint that consumers exercise in the use of personally identifiable information, there are numerous state and Federal laws that govern its use. This includes laws affecting financial, medical and children's information. Our privacy laws have generally focused on regulating the use of sensitive information, rather than attempting to dictate how consumer records are maintained. This American approach of focusing on the areas of greatest concern reflects a careful balancing of consumer interests. A clear distinction should continue to be drawn between what is "personally identifiable information" and what is "non- personally identifiable information."

As a broad principle, ITAA cautions against any regulations which would discriminate against online commerce by establishing requirements not faced in the more traditional brick and mortar economy. Many other studies have linked the productivity gains resulting from the information technology networks as a vital contributor to the long prosperity the country has enjoyed in this decade.

Subj: Online Privacy: Perspectives of Online Privacy Alliance
From: Tim Lordan, 202-638-4371, tim@privacyalliance.org
To: Internet Caucus Advisory Committee

**Layered Approach to Data Privacy Protection
Survey of Regulatory Oversight and Enforcement of Privacy in the US**

The United States has a long history of respecting privacy of Americans. There currently exists numerous laws on the books designed to ensure the privacy of Americans. Some of these restrictions on the collection and use of personal information are based upon how the data is used (FCRA), some on the demographics of the citizen (COPPA), and some on the sensitivity of the data (HIPPA, FSMA). These rules apply online as well as offline. See below for full review.

Layered Approach : In the online world, consumers are afforded additional protections that flow from a layered framework designed to ensure data privacy. This flexible, layered approach starts with publicly announced corporate policies and industry codes of conduct (e.g. Posted privacy policies, publicly endorsed industry codes of conduct via group such as OPA/DMA).

Enforcement : Regulations allow the FTC and state and local agencies to enforce these publicly stated policies on behalf of consumers. With the vast majority of Web sites posting privacy policies, this give these enforcers jurisdiction over just about the whole dot com Internet. In cases where truly bad actors refrain from posting privacy policies in an attempt to avoid enforcement, the FTC has cautioned that “in certain circumstances, information practices may be *inherently* deceptive or unfair, regardless of whether the entity has publicly adopted any fair information practice policies,” leading to the possibility of an FTC enforcement action under section 5 of the FTC Act.

Flexibility : As industry best practices and self-regulatory principles change, FTC’s authority with regard to those practices is already remains in place (no waiting for legislative authority to address issues arising from a new business model).

Successful History : This approach has a long and successful history in the United States. For example, many professions that traditionally have been trusted to safeguard the confidentiality of personal data -- lawyers, doctors, and accountants, for example -- abide by self-regulatory codes backed up by government or judicial enforcement mechanisms, and the result has been a high level of protection that has stood the test of time.

Third Party Enforcement Mechanisms : These enforcement mechanisms provide additional back up to FTC and local enforcement. At present, the OPA endorses several effective “seal” programs (BBBOnLine, CPA Web Trust, ESRB, TRUSTe) and several other enforcement mechanisms (The DMA, IRSG). Thousands of the top sites on the Internet participate in these mechanisms to ensure privacy protections for their consumers.

Teeth in Self Regulation : This layered approach was proven in the GeoCities case, where the FTC challenged the accuracy of certain representations in the website operator’s privacy

policy. The FTC and GeoCities entered into a consent decree in which GeoCities agreed to implement several additional robust privacy practices. GeoCities implemented new practices dealing with information from children – these practices pre-dated COPPA by years. A similar enforcement action was brought against Liberty Financial’s Young Investor site last year. Again, the site’s publicly announced privacy practices were adequately enforced by the FTC.

Survey of Existing Privacy Laws

Many laws addressing industry specific sectors that address the use of personal information exist including:

- the Electronic Communications Privacy Act (ECPA),
- the Fair Credit Reporting Act,
- the Children's Online Privacy Protection Act,
- the Electronic Funds Transfer Act,
- the Video Privacy Protection Act,
- the Telephone Consumer Protection Act of 1991,
- the Cable Communications Policy Act of 1984,
- the Communications Act itself,
- the Financial Services Modernization Act,
- the Federal Aviation Act,
- the Health Insurance Portability and Accountability Act (HIPPA),
- the Right to Financial Privacy Act of 1978,
- a myriad of State law protections.

More Robust Privacy Than Europe :

The sectoral approach to privacy in the US provides much more effective protections than the omnibus approach to privacy that exists within Europe. For example, ECPA, Electronic Communications Privacy Act, provides far more privacy protection to US citizens when they engage in personal and private communications online via email. Through ECPA, the privacy of US citizens is ensured in the most sensitive of Internet communications — via email messages. Email communications between US citizens are protected under this high privacy standard. However, once a US citizen shares personal Internet communications with an EU citizen via email, EU law does not respect ECPA privacy assuring standards on that end of the message.

For more detailed review, see <http://www.privacyalliance.org/news/12031998-5.shtml>

Subj: Online Privacy: Perspectives of Privacy Right
From: Paul Sholtz, Chief Technology Officer, PrivacyRight Inc., c/o Amy Hanson, 703-299-9470
To: Internet Caucus Advisory Committee

What are the legal privacy protections for Internet users?

The 1998 COPPA Act, which protects children's privacy online, is the only significant piece of U.S. legislation concerning Internet privacy. Currently, most privacy violations on the Internet are relatively benign, and are often limited only to behavior tracking for purposes of direct marketing (e.g., DoubleClick). Credit card theft via the Internet is extremely difficult. This is because credit card numbers are protected with SSL at 128 bits which is currently impossible to break. While there is every reason to believe that increasingly serious attacks on privacy could occur on the Internet, the most serious privacy violations remain in the offline world.

Identity theft is the most serious privacy invasion in today's society. However, this is a problem that is perpetuated in the offline world, *not* on the Internet. Identity theft occurs when someone gathers enough personal information on some other individual to assume that person's identity. Often, the criminal will use the Internet to learn personally identifying information about the victim, such as victim's name, address, social security number and mother's maiden name. With this information, the criminal will apply for credit cards using the victim's identity and purchase goods at will, leaving the victim to pay the bill. At present, there are no significant laws against this form of identity theft. When it occurs, the burden of "fixing" the problem lies with the victimized consumer whose identity was stolen. It often takes years for the consumer to reestablish a decent credit rating. It would be more appropriate for the laws to be rewritten so that the burden of absorbing the cost of identity theft lay with the credit card companies, not with consumers.

Subj: Online Privacy: Perspectives of Online Privacy Alliance
From: Tim Lordan, 202-638-4371, tim@privacyalliance.org
To: Internet Caucus Advisory Committee

Excerpt from the Online Privacy Alliance Legal Framework White Paper, See <http://www.privacyalliance.org/news/12031998-5.shtml>

THE FEDERAL TRADE COMMISSION: ENFORCING SELF-REGULATION

Private self-regulatory bodies like the OPA -- which establish a framework of self-imposed data protection rules to govern the conduct of all entities in a given industry that agree to operate according to those standards -- can effectively regulate the behavior of their members and thereby safeguard the private information of consumers. Rather than having to investigate the idiosyncratic information practices of a given company, consumers will learn to associate a prominently displayed seal or notice with a well-known standard of data protection -- much as U.S. consumers today know that the "UL" (Underwriters Laboratories) symbol on electronic appliances¹ guarantees that a device's design meets a time-tested safety threshold. Thus, companies that agree to abide by a recognized self-regulatory standard gain the reputational advantage of being able to advertise a consumer-trusted seal of approval -- and those that do not bear a stigma that can be expected to affect their performance in the marketplace. Internal enforcement mechanisms guarantee that members live up to their promises by threatening violators with the penalty of losing the organization's stamp of approval.

But the efficacy of collective self-regulation in the United States does not depend on the private sector alone. The Federal Trade Commission ("FTC") may use its enforcement authority under section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive trade practices" in interstate commerce, to prosecute companies that do not uphold the standards of a privacy seal or notice that they display for customers. The FTC has broad jurisdiction over companies doing business in the United States as well as substantial enforcement powers. FTC remedies include injunctive relief and other forms of redress and compensation, and thus impose an independent, objective incentive on companies to take industry standards seriously.² State and local consumer protection agencies and consumer advocates, as well as state attorneys general (the latter analogous to the federal Department of Justice), complement the FTC's authority by keeping a watchful eye on regional industries and smaller businesses.

A. The Federal Trade Commission

1. FTC Enforcement Authority

The FTC is an independent administrative agency that has been delegated broad enforcement authority under a variety of statutes designed to promote fair competition and protect the interests of consumers. Certain of these statutes -- like the Fair Credit Reporting Act (discussed below) -- specifically empower the FTC to investigate and prosecute violations of U.S. law governing the treatment of specific types of information

^{1/} The "UL" symbol serves a function similar to the "CE" symbol on products sold in Europe.

^{2/} See Federal Trade Commission, *Individual Reference Services: A Report to Congress* & n.297 (FTC Dec. 1997).

relating to an individual's credit and finances. Others -- like the recently passed Children's Online Privacy Protection Act of 1998 (also discussed below) -- grant the FTC authority to regulate certain data protection practices and dictate minimum standards for the collection and distribution of discrete types of personal information (e.g., data relating to children). More generally, the FTC possesses broad authority under section 5 of the Federal Trade Commission Act to investigate and halt any "unfair or deceptive" conduct in almost *all* industries affecting interstate commerce.³ This authority includes the right to investigate a company's compliance with its own asserted data privacy protection policies. Pursuant to section 5, the FTC may issue cease and desist orders and may also order other equitable relief, including redress of damages.

While the FTC possesses only limited authority to prescribe regulations that have the force of positive law, it *can* determine (subject to judicial review) that a given practice is unfair or deceptive and therefore contrary to the public interest. Furthermore, if the agency through its adjudicatory procedures determines that a given practice constitutes unfair or deceptive conduct (usually in the form of issuing a "cease and desist order"), other parties who engage in similar conduct are subject to civil penalties if they have actual knowledge of the FTC's determination.⁴ Typically, a company will choose not to run the risk of a full-scale FTC investigation and prosecution and will instead enter into a "consent order" with the agency in which a company agrees to comply with objective, judicially enforceable requirements. Thus, the agency often can set a *de facto* minimum standard of behavior through vigorous investigation of companies that engage in questionable conduct, exercising considerable influence over a wide variety of industry practices that the agency deems important to consumers and the public interest. The FTC's recent policy statements and reports leave no doubt that one such area of special concern for the agency is the commercial collection and distribution of personal information.

As demonstrated by the *GeoCities* case (discussed below), the FTC has taken enforcement action to ensure that a company complies with its stated data protection standards.⁵ As companies increasingly adopt and announce privacy policies, therefore, their practices become subject to FTC enforcement. Even where a company has not publicly embraced privacy standards, the FTC has cautioned that "in certain circumstances, information practices may be *inherently* deceptive or unfair, regardless of whether the entity has publicly adopted any fair information practice policies," leading to the possibility of an FTC enforcement action under section 5 of the FTC Act.⁶ For example, prior to the recent adoption of the Children's Online Privacy Protection Act, the FTC issued an opinion letter concluding that "it is likely to be an unfair practice" to collect personal identifying information from children without a parent's prior consent.⁷ As principles of data privacy protection become more ingrained and accepted, other privacy practices similarly could

^{3/} Industries exempt from the FTC's enforcement authority under section 5 are in general subject to specific regulatory schemes that tend to be both comprehensive and rigorous. *See, e.g.*, 47 U.S.C. § 45(a)(2) (exempting banks and savings and loan institutions).

^{4/} *See* 47 U.S.C. § 45(m)(1)(B).

^{5/} *See Privacy Online* at 40 ("[F]ailure to comply with stated information practices may constitute a deceptive practice . . . and the Commission would have authority to pursue the remedies available under the [FTC] Act for such violations.").

^{6/} *Privacy Online* at 40 (emphasis added).

^{7/} *See* Letter from Jodie Bernstein, Director, Bureau of Consumer Protection, Federal Trade Commission, to Center for Media Education, July 15, 1997, available at <http://www.ftc.gov/os/9707/cenmed.htm>.

become sufficiently widespread and expected that a company's failure to comply with such practices -- at least absent notice to consumers -- might be deemed unfair by the FTC.⁸

B. Enforcing Privacy Protection under Section 5 of the FTC Act

A recently settled FTC enforcement action against a website operator demonstrates the FTC's use of section 5 of the FTC Act to assure that companies operate in accordance with their announced information protection practices -- thereby putting teeth in self-regulatory programs.⁹ This represents the FTC's first resolution of a privacy action in the Internet context by way of a consent order, and illustrates the flexibility of existing U.S. law to adapt to new industry sectors in a timely way.

In the GeoCities case, the FTC challenged the accuracy of certain representations in the website operator's privacy notice regarding the use of marketing information collected from persons registering at the site. The FTC's complaint further alleged that GeoCities implied that it operated a website for children without disclosing to the children or their parents that the website was in fact operated by an independent third party. The company denied these allegations but promptly instituted information policies and procedures in accord with standards proposed by the FTC, as ultimately reflected in a proposed consent order.

Under the terms of the consent order, the company agreed to provide clear and prominent notice to consumers of its actual information practices, including what information is collected through its website, the intended uses for that information, any third parties to whom that information will be disclosed, the means by which a consumer may access information collected from herself or himself, and the means by which a consumer may have that information removed from the company's databases.¹⁰ The company agreed that it would not misrepresent the identity of any third party that collects data from a website promoted or sponsored by the company. The company agreed to contact all consumers from whom it previously collected personal information and afford those individuals an opportunity to have data removed from the databases both of the company and any third parties.¹¹

^{8/} State and local consumer protection agencies also scrutinize the extent to which companies engage in deceptive or misleading practices by failing to adhere to announced codes of conduct, and thus provide additional oversight. *See, e.g.*, Cal. Bus. & Prof. Code §§ 17200, 17500 (West 1998) (revised in 1998 to apply explicitly to Internet commerce); N.Y. Gen. Bus. Law §§ 349, 350 (Consol. 1998); *People v. Lipsitz* 663 N.Y.S.2d 468 (N.Y. Sup. Ct. 1997) (applying N.Y. consumer protection statute to false advertising on Internet); Andrew Countryman, "America Online Deal Reached with 44 Attorneys General," *Chicago Tribune* May 29, 1998 (describing deal reached between AOL and state attorneys general regarding AOL business practices). In particular, state and local agencies may be better positioned than the FTC to examine the behavior of smaller and regional companies and to respond to the complaints of individual consumers. *See* John Borland, "States Prepare To Examine New Internet Legislation," *CMP TechWIRE* Jan. 12, 1998 (describing anticipated state legislation to protect Internet consumers). Thus, the enforcement powers and activities of local and state officials and agencies supplements the authority of the FTC and provides an additional layer of protection for personal information.

^{9/} *See In the Matter of GeoCities* File No. 9823015 (FTC 1998); *see also* Michael D. Scott, *GeoCities Targeted by FTC in Internet Privacy Enforcement Action*, *Cyberspace Lawyer* 5-11 (Sept. 1998).

^{10/} At all points at which information is collected, the company must post either this notice or a link informing consumers that data is being collected and directing them to a complete explanation of the company's information practices.

^{11/} The company agreed as well to cease doing business with any third party that refuses to agree to comply with the data removal provisions of the consent order.

Finally, the company agreed to implement procedures to obtain a parent's express consent prior to collecting and using a child's identifying information; moreover, the company may not collect or use a child's identifying information if it has actual knowledge that the child does not have the permission of a parent (or guardian) to disclose that information. The consent order's provisions concerning information gathered from children are virtually identical to those found in the more recently enacted Children's Online Privacy Protection Act.

As a result of this enforcement action, the company must comply on an ongoing basis with the binding rules of conduct specified in the consent order. Beyond that, this highly publicized FTC enforcement action concerning a prominent website operator serves as a benchmark for other companies establishing information practices for their websites.

C. An Industry Model for Facilitating FTC Enforcement of Core Privacy: The IRSG Principles

FTC enforcement is also a powerful tool with respect to enforcement of industry-wide codes of conduct as opposed to company-specific standards or practices. Collective self-regulatory groups can use marketplace dynamics to encourage (or coerce) adherence to a common set of industry "best practices" -- no company can afford to be tarred as a recalcitrant that is unconcerned with the privacy concerns of the public (as illustrated on several occasions in recent years when companies withdrew commercial offerings or practices that were publicly criticized as overly intrusive¹²). Moreover, in contrast to the self-regulatory efforts of individual companies, self-regulatory groups can adopt joint mechanisms to investigate and resolve consumer complaints and thus collectively can enforce each company's compliance with a given industry's best practices. FTC oversight -- in conjunction with that of state and local authorities -- complements such self-regulatory enforcement mechanisms by providing an independent legal incentive for each member company, and the group as a whole, to live up to its promised standard of behavior. The FTC has made clear that, in signing on to an industry group's data protection principles, "a signatory represents that its information practices are consistent with" those principles and that action inconsistent with them subjects a company to liability "under the FTC Act (or similar state statutes) as a deceptive act or practice."¹³

The data privacy standards announced by the Individual Reference Services Group ("IRSG") -- an association of fourteen major companies in the individual reference services industry -- exemplify a self-regulatory approach emphasizing an industry group's seal of approval. The individual reference services industry gathers personal information about individuals from a number of sources, both public (e.g., state driving records) and private (e.g., credit information) and provides that information for a fee to private parties and the government. To protect the often sensitive personal data with which IRSG members deal on a day-to-day basis, the group has adopted binding standards for the protection of personal information. The IRSG developed these rules with the advice and participation of the FTC, and the agency has endorsed them as a promising mechanism to "lessen the risk that information made available through [individual reference] services is misused . . . [and] address consumers' concerns about the privacy of non-public information in the services'

^{12/} See, e.g., *Individual Reference Services* at 1, 13 & n.1 (describing consumer outrage at Lexis-Nexis's "P-Trak" service, which allowed subscribers to identify an individual's social security number; Lexis quickly changed its policies)

^{13/} *Id.* at 29 & n.297.

databases.”¹⁴ The FTC further recommended that the IRSG’s self-regulatory efforts be given an opportunity to demonstrate their effectiveness in conjunction with the FTC’s own enforcement activities (and those of sectoral regulatory authorities).¹⁵

14/ *Id.* at 31.

15/ *See id.*

Online Privacy Part 4: What Are The Legal Privacy Protections For Internet Users (if any)?

Subj: Online Privacy: Perspectives of Progressive Policy Institute
From: Shane Ham, Policy Analyst, Progressive Policy Institute, 202-608-1284, sham@dlcpqi.org
To: Internet Caucus Advisory Committee

In a high profile case last summer, the Federal Trade Commission (FTC), which is authorized to take legal action against companies for “deceptive” practices, did just that against the Internet company GeoCities, which used personal information gathered from its members for purposes other than those it disclosed. Specifically, the FTC charged GeoCities with falsely representing that the personally identifiable records it collects through its membership application form are used only to provide members the specific advertising offers and products or services they request. The FTC further charged that GeoCities falsely represented that “optional,” more detailed personal information collected through the application form is not disclosed to third parties without the members’ permission. In the end, a settlement required GeoCities to post and comply with a more explicitly detailed privacy policy for its members, including greater protection for children under the age of 12, requiring some form of parental consent before children are allowed to give out any personal information.

The basic consumer protection statute enforced by the FTC—Section 5(a) of the FTC Act—declares unlawful any “unfair or deceptive acts or practices” that affect commerce.⁶ Under that statute, the FTC has clear authority to take action against any U.S. Internet site, if, as GeoCities did, it departs from its posted privacy policies, because that amounts to a “deceptive” practice. But federal authority and consumer recourse mechanisms stand on considerably shakier ground when a company doesn’t technically deceive consumers for the simple reason that it doesn’t disclose any sort of privacy policy at all. For the FTC to go after those sorts of Web sites, Congress would need to define what “unfair” practices are in the area of online consumer privacy protection. Unfair practices are currently defined to mean those that “cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” **Note 7**

The FTC reported to Congress in June 1998 that while the vast majority of Web sites of all types collect some sort of personal information—such as name, e-mail address, postal address, phone number, fax number, credit card number, social security number, demographic information, or personal interests—a mere 14 percent of a comprehensive sample of sites openly disclosed some sort of privacy policy or information practice statement. **Note 8** However, close to three out of four of the most popular sites in the survey disclosed either a privacy policy or an information practice statement, or both. And in the year since the FTC’s study, industry-led initiatives encouraging companies to adhere to higher privacy standards have gained momentum.

Presumably, the next FTC-sponsored study, which is to be conducted through Georgetown University, will find some level of improvement in the past year. But the 1998 FTC study’s findings nonetheless underscore an important point about an entirely industry-led approach to privacy concerns: there will always be some companies who choose not to participate in self-regulatory systems.

Note 7 (15 U.S.C. Sec. 45(n)).

Note 8 Federal Trade Commission, “Privacy Online: A Report to Congress,” June 1998.

Subj: Online Privacy: Perspectives of Online Privacy Alliance
From: Tim Lordan, 202-638-4371, tim@privacyalliance.org
To: Internet Caucus Advisory Committee

Excerpt from the Online Privacy Alliance Legal Framework White Paper, See <http://www.privacyalliance.org/news/12031998-5.shtml>

Legal Privacy Protections in US (COPPA, Federal Statutes, State Laws and Common Law Protections)

Children's Online Privacy Protection Act of 1998 (COPPA)

Recently, in response to a study by the FTC concluding that additional regulation was needed to protect the privacy of children, the U.S. Congress enacted the Children's Online Privacy Protection Act of 1998. The Act directs the FTC to promulgate regulations that govern the collection, use, and disclosure of "personal information" obtained online from a child (defined as anyone under the age of 13) by an operator of a commercial website or online service directed to children, as well as any operator with actual knowledge that it is collecting personal information from a child.¹⁶ "Personal information" is defined to include "individually identifiable information," such as a child's name, address, phone number, social security number, e-mail address, or any other "identifier that . . . permits the physical or online contacting of a specific individual."¹⁷ The Act further reaches any other information collected online that is combined with any of the above identifiers.¹⁸ For example, if a website were to assemble a file including a child's name, address, and a list of past purchases, the information about purchases would be deemed subject to the Act.

Congress directed the FTC to promulgate regulations concerning the collection, use, and disclosure of this personal information about children. These regulations must require, *inter alia*, that website and online service providers subject to the Act

- (1) provide notice on the website of what information is collected, how the operator uses the information, and if/when it discloses the information;
- (2) obtain verifiable parental consent for the collection, use, or disclosure of such information;
- (3) permit a parent to obtain any data his/her child has provided to the operator;
- (4) allow the parent to require the operator to delete such data and/or not to collect further data; and
- (5) "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."¹⁹

The Act establishes several narrow exceptions to its reach. For example, its requirements do not apply either to information collected from a child online that is used on a one-time basis

^{16/} Children's Online Privacy Protection Act of 1998, §§ 1302(1), 1303(b)(1).

^{17/} *Id.* § 1302(8).

^{18/} *Id.* § 1302(8)(G).

^{19/} *Id.* § 1303(b)(1).

to respond to a request and is not maintained in retrievable form or to a request for the name of a parent when made for the sole purpose of obtaining consent to collect information about the child.²⁰ The Act also contains a "safe harbor" provision under which an operator is deemed to comply with the FTC regulations if it follows a set of self-regulatory guidelines approved in advance by the FTC (after an opportunity for the public to comment) as meeting the requirements of the FTC regulations.²¹

A violation of the regulations promulgated by the FTC under the Act is deemed to be a violation of Section 5 of the FTC Act,²² the penalties for which are described above. Moreover, the Act provides that certain other specified agencies also shall enforce the Act and the FTC regulations against companies that those agencies regulate; for example, the Department of Transportation must enforce the Act with respect to airlines, and the Federal Reserve Board is charged with enforcement against its member banks.²³ In addition to these forms of federal enforcement, the Act authorizes state attorneys general to bring enforcement actions for injunctive and/or monetary relief for any violation of the FTC regulations.²⁴

Other Federal Statutes that Protect the Privacy of Consumer Information

Numerous other federal statutes also protect the privacy of particular types of information and provide regulatory and/or judicial enforcement mechanisms:

- **Electronic Funds Transfer Act** 15 U.S.C. § 1693 *et seq.* -- This Act requires institutions that provide electronic banking services to inform consumers of the circumstances under which automated bank account information will be disclosed to third parties in the ordinary course of business. The Act is enforced by the Federal Reserve Board, and violations can result in civil and/or criminal penalties.

- **Electronic Communications Privacy Act** 18 U.S.C. § 2510 *et seq.* -- This statute prohibits the unauthorized interception or disclosure of many types of electronic communications, including telephone conversations and electronic mail, although disclosure by one of the parties to the communication is permitted. Violators of this statute are subject to criminal penalties and civil liability.

- **Video Privacy Protection Act** 18 U.S.C. § 2710 -- This statute forbids a video rental or sales outlet from disclosing information concerning what tapes a person borrows/buys or releasing other personally-identifiable information. The Act further requires such outlets to provide consumers with the opportunity to opt out from any sale of mailing lists. The Act is enforced through civil liability actions.

- **Telephone Consumer Protection Act of 1991** 47 U.S.C. § 227 -- This provision mandates that any company making a telephone sales call first consult its list of those who have elected not to receive such calls. The statute grants the Federal Communications Commission ("FCC") the authority to prescribe regulations necessary to protect residential

^{20/} *Id.* § 1303(b)(2).

^{21/} *Id.* § 1304.

^{22/} *Id.* § 1303(c).

^{23/} *Id.* § 1306(b).

^{24/} *Id.* § 1305.

subscribers' privacy rights. The Act also bans unsolicited fax messages. It is enforced by the FCC and through civil suits that can give rise to substantial penalties.

• **The Cable Communications Policy Act of 1984** 47 U.S.C. § 551 *et seq.*, as amended by The Cable Television Consumer Protection and Competition Act of 1992 -- This Act establishes written disclosure requirements regarding the collection and use of personally identifiable information by cable television service providers and prohibits the sharing of such information without prior consent. The Act also provides consumers with the right to access cable company records for purposes of inspection and error correction. The statutory provisions are enforceable through private rights of action for damages.

• **Communications Act** 47 U.S.C. § 222 -- This provision requires telecommunications carriers to protect the confidentiality of customer proprietary network information, such as the destinations and numbers of calls made by customers, except as required to provide the customer's telecommunications service or pursuant to customer consent. These requirements are enforced by the FCC.

• **Federal Aviation Act** 49 U.S.C. § 40101, *et seq.* -- Department of Transportation regulations promulgated under authority of this Act generally require airlines to keep passenger manifest information, such as the names and destinations of passengers, confidential and prohibit use of this data for commercial or marketing purposes.²⁵ These regulations are enforced by the Department of Transportation.

• **Health Insurance Portability and Accountability Act of 1996** 2 U.S.C. § 1301, *et seq.* -- This Act provides that the Secretary of Health and Human Services must promulgate regulations regulating the privacy of individually identifiable health information if Congress itself does not enact legislation on this subject by August 1999. The Secretary has already issued a set of recommendations to Congress that include provisions such as restricting the disclosure of patient identifiable information and providing patients with notice about how such information will be used and to whom it will be disclosed.

• **Office of Thrift Supervision Policy Statement on Privacy** - This policy statement advises savings associations on how to best protect consumer privacy. Among other things, the statement urges savings associations to provide notice to consumers as to how personal information will be used and in what circumstances such information may be disclosed to third parties.

• **Right to Financial Privacy Act of 1978** 12 U.S.C. § 3401, *et seq.* -- This Act mandates that the federal government present proper legal process or "formal written request" to inspect an individual's financial records kept by a financial institution (including a credit card company) and give simultaneous notice to the consumer to provide him/her with the opportunity to object. Both government agencies and financial institutions that violate this Act are subject to civil court actions.

State Law Protection

^{25/} See 14 C.F.R. §§ 243.7, 243.9.

^{26/} Office of Thrift Supervision, *Statement of Privacy and Accuracy of Personal Customer Information* (Nov. 1998).

In addition to sectoral privacy protection at the federal level, states provide both statutory and common law privacy protection with respect to numerous types of data, particularly in the financial and credit sectors. These state laws sometimes complement similar safeguards at the federal level by providing alternative remedies and enforcement schemes. In other cases, the state laws provide protection for types of data that federal laws do not reach.

1. State Statutes

A number of states have statutes that generally concern privacy of financial data. Illinois, for example, regulates the circumstances in which a bank may disclose a customer's financial records, including any information "pertaining to any relationship established in the ordinary course of a bank's business."²⁷ In addition to the state analogues to the FCRA discussed above, a number of state statutes specifically address the use of consumer credit information, particularly for marketing purposes. Maine, for example, generally forbids any sale or disclosure of mailing lists or account information of credit card holders to a third party without an explicit opt-in by the consumer.²⁸ Florida and Hawaii also have opt-in schemes for dissemination of credit card lists, except that they allow disclosures to a third party as long as that party is prohibited from divulging consumer information except to carry out the purpose for which the cardholder provided the information.²⁹ California requires that, before a credit card issuer discloses marketing information to any person, the issuer must inform the cardholder of such disclosure by written notice that provides an opportunity to opt out of the program.³⁰

State statutes also extend privacy protections to other sectors of the economy. A number of states, for example, restrict the collection and disclosure of information gathered by insurance companies. These statutes, based on the Insurance Information and Privacy Protection Model Act promulgated by the National Association of Insurance Commissioners, often require insurance companies and agents to provide a policyholder or applicant notice concerning the types of personal information that may be collected about him or her from a third party and the individual's rights to access and correct information in the company's files.³¹ Many state statutes also protect the privacy of medical information by, for example, providing patients a general right of access to their medical records³² and protection from disclosure of medical records by licensed health-care providers.^{33/}

2. State Common Law

States also provide privacy protection through a number of common law doctrines. On a general level, virtually all states recognize a tort of invasion of privacy. This tort is generally divided into four categories: intrusion upon seclusion of another, appropriation of another's name or likeness, unreasonable publicity given to another's private life, and publicity placing another in a "false light" before the public.^{34/} The most relevant form of this tort in the context of protecting an individual's private data is giving unreasonable publicity to another's private life. Although this tort is unlikely to apply to the

^{27/} Ill. Rev. Stat. ch. 202, § 5/48.1; *see, e.g.*, Minn. Stat. § 13A.01; N.J. Stat. Ann. § 17:16K-3.

^{28/} Me. Rev. Stat. Ann. tit. 9-A, § 8-304.

^{29/} Fla. Stat. ch. 817.646; Haw. Rev. Stat. § 708-8105.

^{30/} Calif. Civ. Code § 1748.12(b).

^{31/} *See, e.g.*, Cal. Ins. Code § 791; Conn. Gen. Stat. Ann. § 38-501; Ill. Rev. St. ch. 215, § 5/1001.

^{32/} *See, e.g.*, Cal. Health & Safety Code § 1795; Colo. Rev. Stat. § 25-1-801.

^{33/} *See, e.g.*, Fla. Stat. chs. 455.241, 395.017.

^{34/} *Restatement (Second) of Torts* § 652A (1977).

disclosure of arguably public information such as names and addresses, release of more private information such as transaction histories might trigger this tort.^{35/}

In certain cases, the relationship between the consumer and the holder of consumer data gives rise to a legally cognizable duty not to disclose consumer information or to do so only in particular circumstances. A number of states, for example, have recognized an implied contractual duty on the part of banks not to disclose information about a depositor's account.^{36/} A similar duty arguably arises in the context of a creditor-debtor relationship^{37/} and a security firm-customer relationship.^{38/}

Finally, state regulation of professionals, such as accountants, doctors, lawyers, and psychologists, often impose restrictions on the use and disclosure of personal information such professionals obtain from their clients. Often the state code simply enforces or supports the self-regulatory code adopted by the profession. For example, many states protect communications between doctors and psychiatrists and patients, recognizing those professions' commitment to safeguarding such communications. Some states also have recognized that accountants have a general duty to maintain the confidentiality of client information.^{39/} State laws often provide additional protections by determining that these professional codes of conduct create fiduciary duties on the part of professionals and permitting civil suits for breach of those duties.

^{35/} *But see Dwyer v. American Express* 52 N.E.2d 1351 (Ill. App. 1995) (rejecting invasion of privacy claim based on alleged sale of card member lists sorted by buying patterns because customers voluntarily used card and company had ownership interest in data).

^{36/} *See, e.g., Barnett Bank of West Florida v. Hooper* 98 So.2d 923, 935 (Fla. 1986); *Twiss v. State Dept. of Treasury* 591 A.2d 913, 919-20 (N.J. 1990).

^{37/} *See, e.g., Pigg v. Roberts* 549 S.W.2d 597, 600 (Mo. Ct. App. 1977).

^{38/} *See, e.g., Barnsdall Oil Co. v. Willis* 152 F.2d 824, 828 (5th Cir. 1946).

^{39/} *See, e.g.,* Alaska Sta. § 8.04.662; Ariz. Rev. Stat. § 32-749; Conn. Gen. Stat. § 20-281j