Attachment 3

Legal Framework White Paper

Submitted with the Comments of the Online Privacy Alliance
On the Draft International Safe Harbor Principles

November 19, 1998

November 19, 1998

OPA White Paper:
Online Consumer Data Privacy in the United States

INTRODUCTION

This autumn marks the entry into force of the European Union's Directive 95/46/EC, which establishes minimum requirements for the protection of personal data across the Community and requires member states to prohibit the transfer of personal data to countries where such data is not subject to adequate safeguards. The Directive takes a broad legislative approach to data protection that is not mirrored in federal and state statutes in the United States. Nevertheless, similar concerns about personal privacy in the digital age affect consumer choices, corporate practices, and, ultimately, legal policies -- governmental, self-regulatory, and judicial -- in the United States. This paper, submitted by the Online Privacy Alliance ("OPA"), illustrates how the collective effect of "layered" regulatory and self-regulatory measures creates "adequate" safeguards for the protection of personal information collected online in the United States.

The OPA is a cross-industry coalition of more than 70 global companies and associations concerned with protecting the privacy of individuals online. As described below, the OPA and its members have adopted standards of conduct tailored to the online environment and intended to ensure that personal information collected online by OPA members receives the level of protection contemplated by the Directive. The OPA has grappled with the unique challenges to and opportunities for data privacy protection that are presented by the enormous and

constant data flow in the online environment and has addressed these in a way designed to reflect the realities of the Internet while satisfying the principles of the Directive and U.S. data privacy policies. The OPA has set forth guidelines for online privacy policies, a framework for self-regulatory enforcement, and a special policy concerning collection of information from children. OPA requires its members to adhere to these guidelines and policies, which are available on OPA's website at http://www.privacyalliance.org.

The layered approach to data privacy protection -- in which publicly announced corporate policies and industry codes of conduct are backed by (a) the enforcement authority of the Federal Trade Commission and state and local agencies; (b) specific sectoral laws that protect the privacy of particular types of information, enforceable by state and federal agencies; and (c) private civil actions for injunctive or monetary relief brought by individuals or classes of consumers -- differs from the comprehensive government regulatory schemes typically used in Europe. Notwithstanding the absence of any regulatory agency dedicated to the enforcement of data privacy standards, however, the "layered" public-private enforcement 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. The framework of self-regulation in the United States, buttressed by the threat of governmental or private enforcement, has succeeded both in protecting personal information and in affording adequate redress to those individuals whose privacy has been invaded. Accordingly, a layered approach -- as adapted to address the unique conditions of the Internet -- should achieve a level of data privacy protection online that satisfies the principles of the Directive.

In recent years the U.S. government has been increasingly concerned about ensuring protection of personal information both online and off. The U.S. government has embraced the layered approach to online data protection and consistently has advocated that self-regulatory efforts -- in the form of industry codes of conduct and self-policing trade groups and

associations -- serve as the primary safeguard to protect the electronic privacy of personal information.[1] This belief in the efficacy of self-regulation reflects U.S. confidence that industry standards will rise to meet the challenge of meaningful data protection, rather than become watered down by a "race to the bottom." Indeed, as discussed below in Part I, the Federal Trade Commission and the U.S. Department of Commerce have identified five key elements of a successful regime for data privacy protection in order to define for U.S. industry the standards the government expects industry to meet:

(1) *notice* of the ways in which information will be used;

(2) *consent* to the use or third-party distribution of information;

(3) *access* to data collected about oneself;

(4) *security* and accuracy of collected data; and

(5) *enforcement* mechanisms to ensure compliance and obtain redress.[2]

Thus, the U.S. commitment to self-regulation presumes-- and will encourage -- the development through industry initiatives of *meaningful* privacy measures that generally adhere to these core privacy principles.

[1/] *See* White House Task Force, *Framework for Global Electronic Commerce* (July 1, 1997).

[2/] *See Privacy Online* at 7-11 (describing principles in detail); U.S. Department of Commerce, *Privacy and Electronic Commerce* (June 1998); *see also* White House Task Force, *Framework for Global Electronic Commerce* (July 1, 1997). The FTC's core privacy principles represent the most recent and comprehensive U.S. effort to identify the fundamental elements of data protection. The FTC framework does not exist in a vacuum, however. The National Telecommunications and Information Agency ("NTIA"), the U.S. Information Infrastructure Task Force, and the Commerce Department each have addressed issues related to the protection of personal information and have all reached similar conclusions as to what constitutes effective data protection. *See Framework for Global Electronic Commerce* (describing results of various studies). The core principles announced by the FTC represent a synthesis of these earlier efforts and the OECD Guidelines. *See* Federal Trade Commission, *Privacy Online: A Report to Congress* 7 & nn. 27. 28 (FTC June 1998), available at http://www.ftc.gov/reports/privacy3.

The U.S. government, furthermore, has made clear that the failure of a company to abide by privacy standards to which it professes to adhere can subject the company to the enforcement authority of the Federal Trade Commission (or of state and local agencies) and consequent legal penalties. This possibility of government enforcement should provide ample incentives for companies to live up to their guarantees of privacy. *See* Part I *infra*. Moreover, as demonstrated in Part II, both federal and state laws provide an additional layer of privacy protection: They establish numerous types of safeguards for data privacy in various sectors of the economy by imposing legal restrictions on the collection and use of particular types of information. These various laws demonstrate the commitment of both the federal and state governments to intervene and protect privacy if self-regulatory efforts in a particular sector need reinforcement.

The OPA privacy guidelines and attendant enforcement mechanisms (discussed in Part III) are designed to work with this regulatory backdrop to protect the privacy of consumers' online data consistent with the principles set forth in the Directive. OPA-prescribed enforcement mechanisms, such as seal programs, provide a means to guarantee that members comply with clearly identified self-regulatory standards. Companies that identify themselves as adhering to the OPA self-regulatory scheme also may be at risk of FTC (as well as state and local) enforcement actions if they fail to follow the OPA privacy principles; many of these companies also will be obligated to comply with various sectoral data protection laws at the federal and state levels. Thus, compliance with the OPA guidelines should provide assurance to EU data protection authorities that personal information collected online will be adequately protected within the United States, and that such protection is enforceable.

OPA and its members have every incentive to adopt strong standards for data protection and privacy. Political, technological, and economic trends are all driving companies to the high end, not the low end, of privacy protection. Recent polls indicate that public concern about online privacy is the number one reason that consumers not currently using the Internet --

still a substantial majority of U.S. consumers -- do not go online,[3] and a substantial number of consumers who do use the Internet choose not to purchase goods sold through websites that do not disclose their privacy policies.[4] Congress and the Administration are well aware of the tide of public opinion, and recent events -- most notably, the rapid passage by the U.S. Congress of the Children's Online Privacy Protection Act -- leave no doubt that the U.S. government will take action if the online industry does not uphold its responsibility to impose meaningful standards for the use and protection of online customer data.

U.S. advocacy of a layered self-regulatory approach to data privacy protection is therefore both a carrot and a stick. Private industry has been given an opportunity to preserve Internet commerce from government regulation -- the carrot. However, if self-regulation does not work, or if industry contents itself with meaningless or self-serving standards, the U.S. government stands ready to impose whatever statutory guidelines are necessary for the successful protection of information gathered online -- the stick.

This emphasis on meaningful self-regulation has produced real progress in the promulgation of substantive guidelines to govern the use of personal information in certain industries. For example, the major players in the growing market for individual reference services ("IRS") -- companies that, for a fee, provide financial and other personal information about individuals -- have worked with the Federal Trade Commission to adopt a code of conduct that imposes strict limitations on the use and sale of personal information by those companies. Similarly, the OPA privacy guidelines demonstrate that the self-regulatory framework outlined by the FTC offers a viable method of protecting personal data collected over the Internet.

[3/] *See Business Week/ Harris Poll: Online Insecurity*, Business Week, Mar. 16, 1998, at 102.

[4/] *See* Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web," before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, July 21, 1998; *Privacy Online* at 3-4.

OPA strongly believes that the interests of its members will best be served by working within that self-regulatory framework to assure the public that personal data will be adequately protected. Online markets are expected to expand dramatically in the coming years, and consumers -- particularly those who have yet to buy products or services online -- have demonstrated that they in fact care a great deal about the privacy policies of the online companies with whom they do business. New technologies, which will allow a consumer to bargain explicitly for a desired degree of privacy protection, will only heighten public awareness of privacy concerns and reinforce the public's expectation that responsible companies will adhere to the privacy principles espoused by OPA today.[5] Internet markets will not reach their full potential until and unless consumers trust that online businesses will not misuse personal data that must be collected to consummate commercial transactions (e.g., shipping addresses, contact information, credit card numbers). Thus, every commercial online business has an incentive to win that trust by safeguarding the privacy of its customer's personal information, and those forward-looking companies that set the standard for data protection on the Internet -- companies like OPA's members -- will earn a competitive advantage in the marketplace.

I. 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

---

[5/] Even today, web browsers can be set to decline "cookies" so as to prevent a website from writing files to a user's disk that permit the site owner to track usage of the website by that user, and filtering programs permit users to prevent access to specified sites, which may include those with unacceptable privacy policies. In the future, automatic protocols like P3P will allow Internet users to negotiate desired levels of privacy protection or to avoid altogether those sites that do not provide sufficient protection for personal information.

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 appliances[6] 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.[7] 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

[6/] The "UL" symbol serves a function similar to the "CE" symbol on products sold in Europe.

[7/] *See* Federal Trade Commission, *Individual Reference Services: A Report to Congress* 29 & n.297 (FTC Dec. 1997).

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 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.[8] 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.[9] 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

---

[8/] 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).

[9/] *See* 47 U.S.C. § 45(m)(1)(B).

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.

2. The FTC's Core Privacy Principles

As noted above, in a June 1998 report to Congress, the FTC identified five core principles of privacy protection that it will deem to represent fair and adequate information practices [10]:

(1) *Notice*: Consumers must be given notice at the time data is collected of (a) what kinds of information are being gathered, (b) whether requests for information may be refused, (c) the uses that will be made of that data, (d) the persons or entities who will receive or have access to that data, (e) the measures taken to ensure confidentiality and accuracy of the data, and (f) whether an individual may limit the dissemination or use of collected personal information.

(2) *Consent*: Individuals should be afforded a choice about the ways in which collected information may be used and whether that information may be distributed to third parties.

(3) *Access*: Individuals should have access to the data that is collected about them and should have some means to correct inaccurate or incomplete information.

(4) *Security*: Companies that collect personal information should take reasonable steps to ensure the *security* and accuracy of that information; in particular, measures should be adopted to prevent unauthorized access to any personal data.

[10/] *See* Federal Trade Commission, *Privacy Online: A Report to Congress* (FTC June 1998), available at http://www.ftc.gov/reports/privacy3.

(5) *Enforcement*: Individuals must have some mechanism to enforce compliance with an objective code of personal information practices and to obtain redress for violations of that standard.

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.[11] 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.[12] 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.[13] As principles of data privacy protection become more ingrained and accepted, other privacy practices similarly could 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.[14]

---

[11] *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.").

[12] *Privacy Online* at 40 (emphasis added).

[13] *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.

[14] 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

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.[15] 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

---

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.

15/ *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).

removed from the company's databases.[16] 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.[17]

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

---

16/ 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.

17/ 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.

as overly intrusive[18]). 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."[19]

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' databases."[20] The FTC further recommended that the IRSG's self-regulatory efforts be given an opportunity to demonstrate

---

18/ *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)

19/ *Id.* at 29 & n.297.

20/ *Id.* at 31.

their effectiveness in conjunction with the FTC's own enforcement activities (and those of sectoral regulatory authorities).[21]

II. SECTORAL REGULATION OF PRIVACY INTERESTS

In addition to the umbrella authority of the FCC over data privacy, the United States has extensive laws regulating the collection and use of consumer data in particular sectors of the economy. This sectoral approach demonstrates the commitment of the U.S. government -- at both the federal and state level -- to regulate the privacy of sensitive data and to step in and provide governmental support for self-regulatory regimes.

A. Principal Federal Statutes

1. Fair Credit Reporting Act

One of the primary federal statutes that protects consumer privacy is the Fair Credit Reporting Act ("FCRA"), which regulates the collection and dissemination of a wide range of information about consumers. The purpose of the FCRA, as articulated by Congress, is "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[22]

In general, the Act regulates the collection and dissemination of "consumer reports," which include information concerning topics such as a consumer's credit worthiness and other personal characteristics, by "consumer reporting agencies" -- any person (or entity) who regularly engages in assembling or evaluating these types of information. Such agencies may disseminate consumer report information only to third parties having a specifically delineated permissible purpose for the information, such as a credit transaction or a determination whether to issue an insurance policy. The FCRA also provides further protections, such as the right of consumers to access and obtain correction of data collected and maintained by consumer

---

21/ *See id.*

22/ 15 U.S.C. § 1681(b) (emphasis added).

reporting agencies. On the other hand, the FCRA also provides certain exceptions to its reach, including, for example, situations in which a merchant makes use of data it obtains based on first-hand experience with a consumer.

The scope of the FCRA's privacy protections is dependent primarily on the definitions of "consumer reports" and "consumer reporting agencies." The FCRA defines "consumer reports" broadly to include "any written, oral, or other communication" to a third party of information "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part" for one of several general purposes.[23] In particular, information bearing on one of the specified characteristics is a consumer report if it is collected, used, or even expected to be used for purposes including credit, employment, insurance, or a legitimate business need in connection with a business transaction with the consumer.[24] Moreover, the collection or use of the information does not have to be only or even primarily for one of these purposes -- it is enough that the information is used, collected, or expected to be used only in part for one of the specified purposes.[25]

This definition of "consumer reports" sweeps a variety of different types of information under the protective umbrella of the FCRA. Data that is collected or used for the purpose of determining credit eligibility or for deciding whether to provide insurance coverage is included.[26] So are reports that are compiled or used to ascertain whether a particular individual is eligible for employment.[27] A list of consumers who have passed bad checks that is supplied to merchants also falls within the category of "consumer reports."[28] The FTC has taken the

---

[23] *Id.* § 1681a(d).

[24] *Id.* §§ 1681a(d), 1681b(a)(3)(F).

[25] *See, e.g., Comeaux v. Brown & Williamson Tobacco Co.*, 915 F.2d 1264 (9th Cir. 1990).

[26] FTC Official Staff Commentary, 16 C.F.R. Pt. 600 app. § 603 item 6.

[27] *Id.*

[28] *See Estiverne v. Saks Fifth Avenue & JBS*, 9 F.3d 1171 (5th Cir. 1993).

position that targeted marketing lists also can constitute "consumer reports" within the meaning of the FCRA.[29]

At the same time, the FCRA does provide certain limitations on the definition of a consumer report. As note above, information does not fall within this category if it is based solely on the disclosing party's first-hand experience with the consumer.[30] Thus, a merchant who discloses the amount and type of its transaction with a consumer is not disseminating a "consumer report" for purposes of the FCRA. This exception may allow dissemination of information without FCRA protection in some circumstances; however, if the recipient of the merchant's firsthand information then sought to pass it on to a third party, the information *would* be protected as a consumer report (assuming, of course, that it met the other requirements of the definition).[31] Recent amendments to the FCRA also provide that information communicated to an affiliated entity is not a consumer report if it was "clearly and conspicuously disclosed" to the consumer that such disclosure might occur and the consumer had the opportunity to "opt out" beforehand.[32]

The FCRA generally regulates the collection and dissemination of "consumer reports" only when done by a "consumer reporting agency." The latter term encompasses any person who for money or on a cooperative nonprofit basis "regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[33] Examples of consumer reporting agencies include credit bureaus such as Equifax, employment agencies that routinely obtain information on job applicants from former employers, tenant screening companies that assist landlords in checking prospective tenants, and check approval companies

---

29/ *See Trans Union Corp. v. FTC*, 81 F.3d 228 (D.C. Cir. 1996) (noting the FTC's position but remanding for further factual development).

30/ 15 U.S.C. § 1681a(d)(2)(A)(i).

31/ FTC, *Compliance with the Fair Credit Reporting Act* 42 (1977).

32/ 15 U.S.C. § 1681a(d)(2)(A)(iii).

33/ *Id.* § 1681a(f).

that guarantee checks for merchants.[34] On the other hand, an entity that gathers or evaluates consumer data on a one-time or other infrequent basis is not subject to the FCRA.

A consumer reporting agency may legally furnish a consumer report to third parties (in the absence of consent[35]) only if it has reason to believe that the third party has one of the permissible purposes listed in the statute. This generally includes someone who requests information in connection with (1) a credit transaction, review or collection of a credit account, or evaluation of a credit application[36]; (2) a determination whether to issue or cancel an insurance policy or how to set the rates and terms of such a policy[37]; (3) a response to a court order[38]; or (4) a legitimate business need in connection with a business transaction involving the consumer (such as renting an apartment or a consumer's offer to pay by check).[39] In addition, a consumer report may be disclosed to a third party for purposes of an employment decision relating to promotion, reassignment or retention, but only if the consumer authorizes such disclosure in writing beforehand.[40] Marketing is *not* a permissible purpose. The consumer reporting agency must maintain reasonable procedures designed to ensure that consumer reports are furnished only for the listed purposes.[41]

The FCRA also provides further restrictions on the dissemination of "consumer reports." For example, a consumer must consent ahead of time to the release of a consumer report for purposes of employment, credit, or insurance if the report contains medical information.[42] The consumer must have the option to opt out of being included in any lists for

---

34/ FTC Official Staff Commentary, 16 C.F.R. Pt. 600 app. § 603(f) items 4, 6(f).
35/ 15 U.S.C. § 1681b(a)(2).
36/ *Id.* § 1681b(a)(3)(A).
37/ *Id.* § 1681b(a)(3)(C).
38/ *Id.* § 1681b(a)(1).
39/ *Id.* § 1681b(a)(3)(E); FTC Official Staff Commentary, 16 C.F.R. Pt. 600 app. § 604(3)(E) item 3.
40/ 15 U.S.C. §§ 1681b(a)(3)(B), 1681b(b).
41/ 15 U.S.C. § 1681e(a).
42/ *Id.* § 1681b(g).

unsolicited credit and insurance offers.[43] The FCRA additionally prohibits the reporting of "obsolete information"; the Act sets forth specific time frames after which particular types of data are deemed obsolete.[44]

The Act further mandates that consumer reporting agencies establish "reasonable procedures to assure maximum possible accuracy."[45] The Act seeks to promote accuracy and reliability in part by creating a framework under which a consumer has the right to obtain the information maintained about him or her and require the consumer reporting agency to correct inaccurate information. Specifically, the FCRA requires that every consumer reporting agency disclose upon request to a consumer the "nature and substance" of the information about the consumer in the agency's files, the sources of that information, and the identity of those who have obtained a report about the consumer in the past year.[46] A consumer may dispute the completeness or accuracy of any information maintained by the agency and require the agency to "reinvestigate" the accuracy of the information at no charge to the consumer.[47] The consumer reporting agency generally must complete such reinvestigations within 30 days.[48] If the agency concludes that the disputed information is inaccurate or unverifiable, it must modify or delete the information.[49] If, on the other hand, the agency decides that the information is accurate, but the consumer continues to dispute that conclusion, the agency must include the consumer's statement of dispute in any subsequent consumer report.[50]

The Act provides a robust enforcement scheme. Consumers can bring civil actions for damages and attorneys fees for negligent or willful violations of the Act.[51] Punitive damages

---

43/ *Id.* § 1681b(e).
44/ *Id.* § 1681c(a).
45/ *Id.* § 1681e(b).
46/ *Id.* § 1681g(a).
47/ *Id.* § 1681i(a)(1).
48/ *Id.*
49/ *Id.* § 1681i(a)(5).
50/ *Id.* § 1681i(c).
51/ *Id.* §§ 1681n, 1681o.

are also available in the case of willful violations.[52] The Act provides for parallel enforcement at the federal level by the FTC, which can bring actions to enjoin further violations and/or to impose civil penalties.[53] Knowing and willful violations of the Act also can lead to criminal penalties, including imprisonment.[54] Finally, most states have analogous credit reporting statutes giving rise to private rights of actions and providing enforcement powers to the state attorney general.[55]

2. Children's Online Privacy Protection Act of 1998

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.[56] "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."[57] The Act further reaches any other information collected online that is combined with any of the above identifiers.[58] 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

---

52/ *Id.* § 1681n(a)(2).
53/ *Id.* § 1681s.
54/ *Id.* §§ 1681q, 1681r.
55/ *See, e.g.*, Cal Civ. Code § 1785 *et seq.*; Conn. Gen. Stat. 36-432 to 435.
56/ Children's Online Privacy Protection Act of 1998, §§ 1302(1), 1303(b)(1).
57/ *Id.* § 1302(8).
58/ *Id.* § 1302(8)(G).

(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."[59]

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 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.[60] 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.[61]

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,[62] 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

---

59/ *Id.* § 1303(b)(1).
60/ *Id.* § 1303(b)(2).
61/ *Id.* § 1304.
62/ *Id.* § 1303(c).

charged with enforcement against its member banks.[63] 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.[64]

3. 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-

63/ *Id.* § 1306(b).

64/ *Id.* § 1305.

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 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.[65] These regulations are enforced by the Department of Transportation.

•*Health Insurance Portability and Accountability Act of 1996*, 42 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*[66] -- 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

---

[65] *See* 14 C.F.R. §§ 243.7, 243.9.

[66] Office of Thrift Supervision, *Statement of Privacy and Accuracy of Personal Customer Information* (Nov. 1998).

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.

B. State Law Protection

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."[67] 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

---

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

credit card holders to a third party without an explicit opt-in by the consumer.[68] 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.[69] 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.[70]

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.[71] Many state statutes also protect the privacy of medical information by, for example, providing patients a general right of access to their medical records[72] and protection from disclosure of medical records by licensed health-care providers.[73/]

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,

---

68/ Me. Rev. Stat. Ann. tit. 9-A, § 8-304.

69/ Fla. Stat. ch. 817.646; Haw. Rev. Stat. § 708-8105.

70/ Calif. Civ. Code § 1748.12(b).

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

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

73/ *See, e.g.*, Fla. Stat. chs. 455.241, 395.017.

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.[74/] 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 disclosure of arguably public information such as names and addresses, release of more private information such as transaction histories might trigger this tort.[75/]

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'saccount.[76/] A similar duty arguably arises in the context of a creditor-debtor relationship[77/] and a security firm-customer relationship.[78/]

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.[79/] State laws often provide additional protections by

---

74/ *Restatement (Second) of Torts* § 652A (1977).

75/ *But see Dwyer v. American Express*, 652 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).

76/ *See, e.g., Barnett Bank of West Florida v. Hooper*, 498 So.2d 923, 935 (Fla. 1986); *Twiss v. State Dept. of Treasury*, 591 A.2d 913, 919-20 (N.J. 1990).

77/ *See, e.g., Pigg v. Robertson*, 549 S.W.2d 597, 600 (Mo. Ct. App. 1977).

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

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

determining that these professional codes of conduct create fiduciary duties on the part of professionals and permitting civil suits for breach of those duties.

III. THE ONLINE PRIVACY ALLIANCE: USING SELF REGULATION TO SAFEGUARD CONSUMER PRIVACY ONLINE

In keeping with the traditional commitment to self regulation in the United States and in response to the FTC's and the Clinton administration's call for responsible self-enforcement of privacy protection by U.S. industry, many U.S. businesses have come together to begin exploring the creation of self-regulatory programs. One particularly successful example of this effort has been the OPA, which brought together over 70 leading global companies and associations beginning in 1998 to address growing public concern over online privacy issues.

The online medium creates particular challenges for privacy protection while simultaneously creating significant opportunities for consumer privacy education and empowerment. The challenges are manifold: Use of the Internet necessarily involves a tremendous flow of information, much of it personal in nature, in a wide variety of contexts. Some information flows involve the consumer actively providing information. For example, commercial Internet transactions require consumers to provide credit card or other payment and contact information, and in certain more sensitive contexts, some transactions may require other identifying data. Some sites may seek data in order to satisfy the consumer's request for information or services, such as where a consumer is asked about family size or smoking habits in response to an inquiry about hotel accommodations. Other sites may request data simply to use for marketing purposes. Consumers also may provide a great deal of data in order to obtain personalized services, such as targeted clipping services or personalized Internet service offerings. In some cases, consumers provide data without necessarily realizing they are doing so. For example, simply visiting or subscribing to certain online sites or services may itself create a footprint that conveys data about the individual's interests. But regardless of the

context, all data collected online is already in digital format, which makes it easy to manipulate, store, and process, and in turn provides massive capabilities for use and transfer of data. Meanwhile, unless effective security measures are used, collection of data online is susceptible to computer "hacking" by unauthorized users, and also to fraud by consumers posing as a third party.

These challenges place a special obligation on the online industry to educate consumers about the Internet's privacy risks and to enhance consumers' ability to make educated choices about how to protect their privacy rights. And indeed, the online medium provides tremendous opportunities for consumer data protection. Online merchants have an unmatched ability to provide consumers with information online quickly, efficiently, and cheaply. Unlike offline merchants who must rely on a one-time mailing or a small print notice in a catalogue, online merchants (or other site owners) interact directly with the consumer each time the consumer visits the merchant's site and therefore have the opportunity to educate and interact with the consumer concerning the site's privacy policies before any data collection takes place. Where appropriate, therefore, consumer consent can be requested at the point where a consumer interacts with a site or inquires about a product or service. Moreover, the merchant's ability to control what the consumer sees on any page of its site provides the merchant with a unique ability to educate the consumer about the site's privacy policy. The site can emphasize its participation in a privacy seal program, for example, or provide a link to the site's privacy policy from any page of the site. This in turn can empower consumers to make educated choices about whether they wish to deal with the particular online service based, at least in part, on the level of privacy protection the online operator provides.

The online environment also permits a site to be designed to permit different levels of participation (or provide different types of benefits) based on the consumer's willingness to provide information, or to provide different levels of protection based on

consumer demand. Online services also may provide the ability to make data anonymous easily, or to do so selectively upon consumer request. In addition, new technologies, such as P3P and filtering programs, provide consumers with the means to exercise independent control over the level of privacy they obtain while online. Finally, consumers have the ability to vary the level of privacy protection they desire each time they visit an online service or site: The process for providing or withdrawing consent is accessible and can be executed immediately and repeatedly to personalize the level of privacy protection.

Thus, if the online industry takes seriously its obligation to educate and inform consumers, the medium presents enormous opportunities for consumer choice and self-determination. Accordingly, a central pillar of OPA's self-regulatory program is the requirement that an online site notify consumers about the site's data collection and dissemination policies. OPA members are committed to providing consumers with the information and tools they need to make informed choices. A second pillar of OPA's program is ensuring that consumers have the opportunity to make choices: consumers must be able to consent or withhold consent to the use of their data by the site they visit. Lack of consent may manifest itself in the consumer's refusal to use the particular service or continued interaction with the site on a limited level. In some cases, consent or opt-out may be more explicit and permit consumers to participate in the site while blocking only certain secondary uses of the consumer's data.

OPA's program is designed to address the challenges and opportunities provided by the online medium while addressing the U.S. government's and the Directive's data privacy concerns. OPA has adapted these privacy principles to address the Internet industry's enormous, ongoing data flows. In order to enforce the OPA's privacy program and policies, the OPA encourages participation in a seal program that will ensure and enforce a minimum standard level of privacy protection. The seal program must also be easy for consumers to recognize and understand. Seal programs provide the added benefit

of being backed up by the FTC's umbrella enforcement authority, state and local consumer protection agencies, and applicable sectoral data privacy regulation.

A. OPA's Privacy Policy Guidelines

In keeping with the key substantive requirements of the Directive and the FTC's privacy principles, the OPA's privacy program addresses notice to data subjects, limitations on use of data, data security and quality, the right to correct personal data, and onward transfers of data. The OPA's program for online data privacy protection is compared with the key requirements of the Directive below.

Notice to Consumers. Because of the rapidly growing ability to collect data about online consumers and the increasing demand for a personalized browsing experience, OPA strongly believes that website operators have a heightened responsibility to make available to online consumers the information necessary to make informed decisions about data privacy. The OPA believes that properly informed consumers should then be allowed to choose the level of privacy that they desire. The OPA therefore requires its members to post a privacy policy that online consumers can view before or at the time that personal data is collected or requested. The privacy policy must, among other things, notify consumers about the online site's data collection practices. The OPA's privacy policy requirement thus is similar to Article 10 of the Directive, which requires data controllers to provide data subjects with information about the controller's identity, the purposes of data processing, and other information necessary to guarantee fair processing. In addition, the privacy policy must be easy to find, read and understand; it also must clearly describe the information that is being collected, any possible onward transfers of personal data, and any options that consumers have to refuse to provide data or to block certain uses or transfers of data. OPA further encourages its members to disclose in their privacy policy any consequences of a consumer's refusal to provide information, the accountability or enforcement mechanism(s) used by the organization, and information about how to contact the organization with privacy concerns. By

requiring members to provide comprehensive online privacy policies that are easy to find and read, OPA ensures that all online consumers have the information necessary to make an informed decision about whether or not to provide personal information to particular websites, how much information to provide, or whether to even visit certain sites.

Limitations on purposes and onward transfers. Consistent with the OPA's principles regarding notice and consent, the OPA advocates allowing data subjects to opt out of any uses or processing unrelated to the original purpose for which the data are collected. Like Article 6 of the Directive, which requires that personal data not be further processed in a way incompatible with the original purpose for collecting the data, the OPA privacy guidelines limit the extent to which data can be processed for purposes unrelated to the original disclosed purposes in the absence of proper consent. The OPA guidelines similarly limit transfers to third parties for marketing purposes or for other purposes unrelated to the original purposes for collecting the data, much like Articles 10 and 11 of the Directive, which require notifying data subjects of onward transfers of data to third parties where notification is necessary to ensure fair processing of the data. With respect to disclosure of data for marketing purposes, OPA requires its members to disclose in their privacy policies possible onward transfers of personal data and any marketing uses of data. These requirements, and the consumer's ability to leave the site or, in some cases, to opt out of a specific data use on the site, address the principles in Article 14 of the Directive, which provides data subjects with the right to notice prior to disclosure of their personal data for direct marketing purposes and the right to object to direct marketing uses of their data. OPA also encourages its members to take reasonable steps to ensure that third party transferees take reasonable precautions to protect transferred data.

Data quality, access to data, and correction. The OPA supports the Directive's principles of assuring that 1) data are accurate, complete, and timely for their intended purposes, and 2) consumers can access data about them and correct that data where

appropriate. However, the extraordinarily wide range of online data processing activities makes it difficult and costly to require all websites to provide consumers with unrestricted access to personal data without regard for its intended purposes or alternative means of ensuring that individuals are informed of data collection and that data quality is maintained as appropriate to those purposes.

Consistent with the spirit of Article 12 of the Directive, which guarantees data subjects the right to access personal data and have that data corrected where necessary, the OPA requires its members to provide "easy mechanisms" for consumers to make inquiries and lodge complaints or objections. The precise mechanisms for such inquiries and the nature and scope of information provided to the consumer on request will necessarily vary according to the data at issue and the costs and benefits associated with furnishing access to the raw data or a summary of the data, given the context of the specific intended uses of the data. For example, some data collected online may be used for electronic commerce transactions or decisions to provide or terminate a service. OPA anticipates that its members would routinely provide access to transaction records and an opportunity to lodge corrections, as these have a substantive impact on the consumer. By contrast, a website may automatically record navigational or "clickstream" data as an individual moves from page to page on a site, either for statistical purposes (to better design and manage the site) or to automatically personalize the initial pages presented to the visitor based on the visitor's historical use of the site. Such information is processed automatically and changes over time. There is little benefit, and much cost, in accumulating this data in a form that could be reviewed intelligibly by the individual at any moment. Moreover, doing so raises additional privacy risks, since it means that more data is readily retrievable by name, and more identifying data must be collected to ensure that the person requesting access is indeed the data subject. Similarly, the use of website data to determine automatically whether to send an individual a product solicitation involves no substantive decision that affects significant consumer interests and does not

warrant the cost (and sometimes the increased privacy risks) of storing and providing subsequent access to the data that prompted the solicitation.

Because the online medium entails the possibility of tracking and recording enormous amounts of data on the use of a website, the costs of furnishing unlimited consumer access to all such data would often be prohibitive. The data may not be maintained in a manner conducive to consumer-specific access: marketing data, for example, is often coded and stored by categories of merchants or purchases rather than by consumer. Before imposing on website operators (and ultimately on consumers) the costs of providing access to all data resulting from a site visit, the nature and uses of that data must be taken into account. Where data is not used for a purpose that in any way affects the consumer's "fundamental rights or freedoms," or that does not even involve denial of a more mundane benefit to the consumer, the cost and difficulty of access must be given particular weight.

Access by the individual to all data generated online is not the only means of ensuring that consumers (and the relevant enforcement bodies) are aware of the operator's data collection practices and can assess their potential impact. This can often be accomplished, for example, by appropriate notices, consumer education, and monitoring techniques such as the use of "decoys" (pseudonymous registrations to check the manner in which an online service or website uses personal data), rather than by individualized access to vast amounts of non-sensitive data. It is in the nature of online services and websites that it is easy to display notices at the point where information is collected and to give visitors an opportunity at any stage to seek clarification, opt out, or simply leave a site if they are not satisfied with its privacy practices. This offers an efficient means of protecting privacy and should suffice where the data collection is not used for substantive decisionmaking.

Security. Like Article 17 of the Directive, the OPA advocates taking appropriate measures to protect personal data from destruction, loss, misuse or alteration.

Collection of data from children. Well before the passage of the Children's Online Privacy Protection Act, discussed above, the OPA thought it necessary to provide special protection for young Internet users. Out of this concern, the OPA was among the first organizations to adopt principles specifically addressing collection of data from children under the age of 13. These specific principles require OPA members to obtain prior parental consent before collecting any individually identifiable offline contact information from children under the age of 13. Members may collect online contact information from children without obtaining prior parental consent only if they notify parents and allow them to prevent use of the data. Other special protections provided by these OPA principles include requiring members to prevent children from being able to publicly post individually identifiable contact information without prior parental consent; prohibiting members from using special games, prizes or activities to entice children to reveal more information than necessary to participate in the activity; and prohibiting members from distributing to third parties any individually identifiable information collected from a child without obtaining prior parental consent.

B. Enforcement Mechanisms

Although membership in the OPA, standing alone, itself denotes a commitment to privacy protection that arguably could be enforced by the FTC, OPA also advocates that its members commit to an independent enforcement mechanism intended to back up that commitment. OPA promotes participation in a "seal program" by its members as a means of enforcing the OPA privacy guidelines and the member's privacy policies. Seal programs provide participants the right to use an identifiable symbol or logo ("seal") to alert consumers that the participant's online service complies with the seal program's standards; that the participant has procedures to ensure compliance; and that the participant participates in a program designed to resolve consumer complaints.

Seal programs are ideal enforcement mechanisms in the online environment for two reasons. First, seal programs take advantage of the visual nature of websites to alert

consumers' attention to privacy policies and practices through the use of visible and easily recognizable graphic seals that can, if desired, be displayed on every page of a site. Second, to some extent seal programs standardize the terms and terminology of privacy practices, making them easier for consumers to comprehend. They give consumers a relatively simple, user-friendly means of identifying websites that have made privacy commitments, linked to greater detail about the site's particular practices.

In many seal programs, participants cede a degree of investigative or complaint resolution authority to the seal program's enforcement entity. The entity often is permitted to disclose complaints to the public and government agencies, and the entity can drop a company that fails to conform with the required conduct. Moreover, seal programs may provide government agencies with a hook to mix self-enforcement with government regulation: as discussed in Part I above, a company's public affirmation of participation in a seal program would provide the FTC (or other consumer protection entity on the state or local level) with the grounds to prosecute a company's failure to in fact uphold the standards articulated by the seal program.

A seal program meeting OPA's criteria would enhance data privacy protection by requiring that seal participants live up to the types of privacy guidelines advocated by OPA, as well as any additional policies the seal program adopts. OPA does not, at least currently, intend to operate its own seal program, and it has not endorsed a specific program to date. In reviewing seal programs, however, OPA would expect a commitment to at least the same degree of privacy protection espoused by the OPA, as well as the following enforcement practices and policies:

Participation from outside the business community. OPA suggests that the seal program obtain input from representatives of consumer advocate groups and academia, in addition to representatives of the business community.

Verification and monitoring. Prior to awarding the seal to an organization, the seal program must require participants to submit to a compliance review by the seal program

or provide a self-assessment verifying that the organization is in compliance with the program's standards. Once the seal has been awarded, participants must consent to periodic verification in the form of auditing, periodic reviews, or use of pseudonymous "decoys" or other technological monitoring.

Complaint resolution. The seal program must require participants to provide an easy-to-use consumer complaint resolution process that will serve as the consumer's first remedy. If the participant and consumer are unable to resolve a complaint through the participant's internal dispute resolution process, the participant must then submit to the seal program's complaint resolution mechanism. In addition to these mechanisms, consumers must not be prohibited from pursuing any other legal remedies that may be available to them under federal or state law.

Penalties for noncompliance. Failure to comply with the requirements of the seal program (and in particular, failure to follow the program's dispute resolution requirements) should result in placing the participant on probation or instituting proceedings to revoke the participant's right to use the seal.

Monitoring for misuse or misappropriation. The seal program should monitor use of the seal and if necessary, bring litigation to prevent unauthorized use of the seal. In addition, the seal program must refer non-complying companies to appropriate government agencies, including the FTC.

Education and outreach. The seal program must educate consumers and businesses about the seal program and online privacy issues. These education and outreach efforts should include providing publicity for participants, publicly disclosing seal revocation and material non-compliance, and periodically publishing verification and monitoring procedures.

To date, two major seal program initiatives are underway or about to be launched that may embody the policies and practices advocated by the OPA: TRUSTe and BBB*OnLine*. The OPA is monitoring the development of those programs and others to

determine whether they meet OPA's requirements for privacy protection and effective enforcement.

The TRUSTe program, which began as a collaboration between the Electronic Frontier Foundation and CommerceNet, has been administering its online privacy seal program since June of 1997. This program requires participants to post an online privacy policy that meets TRUSTe guidelines, to submit to TRUSTe oversight, and to cooperate with TRUSTe's dispute resolution efforts. In return, participants are given the right to display TRUSTe's seal on their home page. This seal serves as a link to the company's privacy policy, and consumers can also verify the authenticity of the seal online.

The privacy policy required of TRUSTe participants must explain what data are being collected, the purposes of data collection and processing, with whom the data will be shared, the consumer's options concerning processing and onward transfers, data security procedures that are in place, and how consumers can update or correct data. Licensees who join or renew after October 1998 must also give consumers the opportunity to opt out of secondary or third-party uses of data provided by the consumer. Also in October 1998, TRUSTe introduced a Children's Privacy Seal Program that applies to websites directed specifically at children under the age of 13, as well as sites that collect age-specific information. The children's program requires site operators to notify parents and obtain their consent before collecting and using a child's online or off-line contact information. Sites aimed specifically at children must post the unique "kid's seal."

TRUSTe utilizes a variety of verification and enforcement techniques. In cases where TRUSTe suspects that a participant is not complying with program guidelines or with the participant's own privacy policy, the participant may be subject to on-site compliance reviews by TRUSTe's official auditors, revocation of the right to use the TRUSTe seal, termination from the TRUSTe program, and referral to appropriate government agencies.

The Better Business Bureau ("BBB") runs the largest and most recognized retail, service and national advertising self-regulation and consumer dispute resolution programs in the United States. Using its self-regulatory models as a starting point, the BBB has been operating an online seal program (with more than 2000 participants) through BBB*OnLine* since mid-1997. BBB*OnLine* assists consumers in finding reliable online merchants that have agreed to BBB standards for truthful advertising and customer satisfaction. BBB*OnLine* has proposed a privacy program that likely will be similar in many ways to the TRUSTe program and will utilize *BBBOnLine*'s existing self-regulatory framework.

BBB*OnLine* is still in the process of developing its privacy principles. These principles are expected to be similar to those of the OPA and TRUSTe programs, although they may in some respects provide additional privacy protections not currently required by the OPA and TRUSTe. The BBB*OnLine* enforcement framework will consist of use a recognizable seal to assert compliance with BBB*OnLine* principles and the company's privacy policy, a comprehensive annual compliance assessment, additional independent verification measures, consumer dispute resolution, and appropriate referrals by BBB*OnLine* to the FTC and other government authorities. BBB*OnLine* participants will have to respond promptly to all consumer complaints, submit to BBB*OnLine*'s dispute resolution process, and maintain a satisfactory complaint handling record with the BBB. BBB*OnLine* will refer eligible complaints to a free, informal dispute resolution process patterned after BBB's national advertising review program, and BBB will make that process available for complaints about non-seal participants as well as seal participants. BBB*OnLine* also will refer uncooperative or non-compliant companies to the FTC or other appropriate federal or state regulatory agencies.

IV. Conclusion

As Articles 25(2) and 27 of the Directive make clear, the EU has recognized that industry and professional standards can be powerful tools for protecting data privacy. In the United States, industry-wide self-regulation of data privacy can be an especially effective means of ensuring that consumer data receives the level of protection embodied in the EU Directive where such self-regulation combines private sector standards with FTC enforcement, regulation by federal and state agencies and, where appropriate, enforcement by the courts.

In the online environment, OPA has established principles -- principles its members must publicly embrace -- that are consistent with the policies of the U.S. government and with the Directive. OPA members must submit to dispute-resolution procedures, and, by publicly embracing OPA's principles, members are also subject to potential enforcement by the FTC and other government agencies. The emergence of two online privacy seal programs demonstrates that the enforcement element of OPA's self-regulatory framework is not just hypothetical, but is quickly developing. Moreover, these seal programs are not engaging in a "race to the bottom," but rather, in keeping with the recent initiatives and pronouncements of the U.S. government, they are embracing meaningful principles embodying a significant degree of privacy protection. In addition, OPA members frequently will be subject to additional regulation of various types of data protection on both the state and federal level, enforced by government agencies and the courts. Self-regulatory programs such as OPA's, which are designed to operate in the context of the United States' layered approach of self-regulation backed by government enforcement, should be recognized as effective by the EU in its effort to protect privacy while promoting the uninterrupted flow of global commerce.

W. Scott Blackmer (sblackmer@wilmer.com)
Lynn Charytan (lcharytan@wilmer.com)

Wilmer, Cutler & Pickering

Washington, DC