Fair Information Practice Principles

EDIT

Contents

Introduction

> *The FIPPs address the collection and use of personal information, data quality and security, and transparency, among other things, and have served as the basis for many of the privacy recommendations federal agencies have made.*[1]

The **Fair Information Practice Principles** (**FIPPs**) are a widely accepted framework that is at the core of the Privacy Act of 1974 and is mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. "FIPPs are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other interests."[2]

The concept of defining principles to be used in the evaluation and consideration of systems, processes, or programs that impact individual privacy is not a new one. In his seminal work, *Privacy and Freedom,* published in 1967, Professor Emeritus Alan Westin identified a number of "criteria for weighing conflicting interests."[3]

HEW Report

The FIPPs were first articulated in a comprehensive manner in the U.S. Department of Health, Education and Welfare's seminal 1973 report entitled Records, Computers and the Rights of Citizens (1973) (full-text) (hereinafter "HEW Report"). The HEW Report was the result of the committee's look at the impact of computerization of information on privacy and included recommendations on developing policies that would allow the benefits of computerization to go forward, but at the same time provide safeguards for personal privacy.

The backdrop surrounding the HEW report and the Privacy Act of 1974 included several years of intense Congressional hearings examining the surveillance activities of the Nixon and J. Edgar Hoover era and the post-Watergate support for government reform.[4]

In the HEW Report, the Advisory Committee recommended the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems and set forth five basic principles to safeguard requirements for automated personal data systems:

- There must be no personal data record-keeping systems whose very existence is secret. (transparency; openness)
- There must be a way for an individual to find out what information about him or her is in a record and how it is used. (individual participation)

- There must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent. (purpose limitation)
- There must be a way for an individual to correct or amend a record of identifiable information about him or her.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. (data quality and integrity)

The Code of Fair Information Practices predated the Privacy Act of 1974 by over a year, and influenced the enactment of the Privacy Act.

From their origin in 1973, fair information practices "became the dominant U.S. approach to information privacy protection for the next three decades."[5] Since the HEW Report, a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies.

European Developments

A number of European countries also began to build upon the HEW principles and individually enacted omnibus data protection laws. In 1980, the international Organization of Economic Cooperation and Development (OECD) codified its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The original five principles set forth in the HEW Report were extended in the OECD guidelines that govern "the protection of privacy and transborder data flows of personal data" and include eight principles that have come to be understood as "minimum standards . . . for the protection of privacy and individual liberties."[6]

The OECD Privacy Guidelines are the most widely-accepted privacy principles, and they were endorsed by the U.S. Department of Commerce in 1981.[7] The OECD Fair Information Practices are also the foundation of privacy laws and related policies in many other countries, (e.g., Sweden, Australia, Belgium).[8]

In 1995, a variation of these principles became the basis of the EU Directive on the Protection of Personal Data. The FIPPs have also been agreed upon by OECD member countries, including the United States, through a consensus and formal ratification process and form the basis of many modern international privacy agreements and national laws.

The OECD Privacy Guidelines were reaffirmed by the OECD in a 1998 declaration and further endorsed in a 2006 report.[9]

In 2004, the FIPPs were championed again by the United States in the development of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. In 2004, the Chief Information Officers Council issued the "Security and Privacy Profile for the Federal Enterprise Architecture" that links privacy protection with a set of acceptable privacy principles corresponding to the OECD's Fair Information Practices.

U.S. statutes

The FIPPs have also formed the basis of many individual laws in the United States, at the both federal and state levels, including the:

- Fair Credit Reporting Act of 1970
- Privacy Act of 1974
- Right to Financial Privacy Act of 1978
- Electronic Communications Privacy Act of 1986
- Video Privacy Protection Act, and
- Children's Online Privacy Protection Act

Many states have incorporated these principles in their own state laws governing public records and in some instances private sector data as well. A number of private and not-for-profit organizations have also incorporated these principles into their privacy policies.

Homeland Security Act of 2002

Section 222 of the Homeland Security Act of 2002, *as amended,* which is the basis for the authorities and responsibilities of the DHS Chief Privacy Officer, also recognizes the significance of the FIPPs. This section calls on the Chief Privacy Officer to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974." Pursuant to Section 222, the DHS Privacy Office has used the FIPPs to assess privacy when conducting Privacy Impact Assessments, issuing System of Records Notices, and developing privacy policies for the Department. The FIPPs provide the foundation of all privacy policy development and implementation at the Department and must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status.

Major reports setting forth FIPPS

In addition to the HEW Report, the major reports setting forth the core fair information practice principles are:

- The Privacy Protection Study Commission, Personal Privacy in an Information Society (1977) [hereinafter "Privacy Protection Study"] (full-text).
- Organization for Economic Cooperation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) (hereinafter "OECD Guidelines") (full-text). The following table identifies the Fair Information Practice Principles as set forth in the OECD Guidelines:

Table 1: The Fair Information Practices

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organization for Economic Cooperation and Development.

- Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (1995) [hereinafter "IITF Report"] (full-text).
- U.S. Department of Commerce, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (1995) [hereinafter "Commerce Report"] (full-text).
- The EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (1995) [hereinafter "EU Directive"] (full-text).
- The Canadian Standards Association, Model Code for the Protection of Personal Information: A National Standard of Canada (1996) [hereinafter "CSA Model Code"] (full-text).
- The Asia-Pacific Economic Cooperation (APEC) Privacy Framework (full-text).
- OECD, Making Privacy Notices Simple: An OECD Report and Recommendations (July 24, 2006) (full-text).

The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.[10]

Core Principles

Common to all of these documents (hereinafter referred to as "fair information practice codes") are five core principles of privacy protection:

(1) Notice/Awareness;
(2) Choice/Consent;
(3) Access/Participation;
(4) Integrity/Security; and
(5) Enforcement/Redress.

The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Striking that balance varies among countries and among types of information (e.g., medical, employment information).

Notice/Awareness

The most fundamental principle is "notice" (now often referred to as "transparency.")

> [C]onsumers should be given clear and conspicuous notice of an entity's information practices before any personal information is collected from them, including: identification of the entity collecting the data, the uses to which the data will be put, and the recipients of the data; the nature of the data collected and the means by which it is collected; whether provision of the requested data is voluntary or required; and the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.[11]

Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.[12] Moreover, three of the other principles discussed below — choice/consent, access/participation, and enforcement/redress — are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.[13]

While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- identification of the entity collecting the data;[14]
- identification of the uses to which the data will be put;[15]
- identification of any potential recipients of the data;[16]
- the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);[17]
- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information;[18] and
- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.[19]

Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data; whether the consumer has been given a right of access to the data;[20] the ability of the consumer to contest inaccuracies;[21]the availability of redress for violations of the practice code;[22]and how such rights can be exercised.[23]

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

Choice/Consent

The second widely-accepted core principle of fair information practice is consumer choice or consent. Virtually every set of fair information practice principles includes consumer choice or consent as an essential element. [24]

> “Under the choice principle, data collectors must afford consumers an opportunity to consent to secondary uses of their personal information, such as the placement of a consumer’s name on a list for marketing additional products or the transfer of personal information to entities other than the data collector.[25]”

Specifically, choice relates to secondary uses of information — *i.e.,* uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer.[26] Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put.[27] Thus, for example, consumers can be provided separate choices as to whether they wish

to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a website, thus effectively eliminating any need for default rules.[28]

Access/Participation

Access is the third core principle. It refers to an individual's ability both to access data about him or herself — *i.e.,* to view the data in an entity's files -- and to contest that data's accuracy and completeness.[29] Both are essential to ensuring that data are accurate and complete.

Access is essential to improving the accuracy of data collected, which benefits both data collectors who rely on such data, and consumers who might otherwise be harmed by adverse decisions based on incorrect data. It also make data collectors accountable to consumers for the information they collect and maintain about consumers, and enable consumers to confirm that websites are following their stated practices.

To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.[30]

Integrity/Security

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.[31]

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.[32] Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.[33]

Security is a process: no one static standard can assure adequate security, as threats, technology and the Internet itself are constantly evolving. Commercial websites should maintain security programs to protect personal data and that data security requirements may vary depending on the nature of the data collected. Each website should maintain a security program that is "appropriate to the circumstances."

Enforcement/Redress

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.[34]Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.[35]

Self-regulation

To be effective, self-regulatory regimes[36]should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress).[37]Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association;[38]external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue.[39]A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.[40]

Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.[41]Thus, a self-regulatory

system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.[42]

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (*e.g.,* correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer.[43] Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

Private Remedies

A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation.[44] The creation of private remedies would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information. Important questions would need to be addressed in such legislation, *e.g.,* the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages;[45] and the elements of any such cause of action.

Government Enforcement

Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers.[46] Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.[47]

References

1. ↑ Vehicle Data Privacy, at 9 n.21.
2. ↑ In-car Location-based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers, at 25 n.4.
3. ↑ These principles were included in chapter 14 of *Privacy and Freedom,* entitled "Restoring the Balance of Privacy in America."
4. ↑ Flowing from the numerous abuses of power uncovered by Congress and the media during the early 1970s, the Privacy Act of 1974 set out a comprehensive regime limiting the collection, use and dissemination of personal information held by government agencies. The Privacy Act of 1974 also established penalties for improper disclosure of personal information and gave individuals the right to gain access to their personal information held by Federal agencies.
5. ↑ Alan Westin, Social and Political Dimensions of Privacy 436 (2003).
6. ↑ Marc Rotenberg, The Privacy Law Sourcebook 2001, at 270-72 (Electronic Privacy Information Center) (2001).
7. ↑ Report on OECD Guidelines Program, Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce (Oct. 30, 1981), *as cited in* Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information.
8. ↑ *Id.*
9. ↑ OECD, Making Privacy Notices Simple: An OECD Report and Recommendations (July 24, 2006).
10. ↑ Such principles can be either procedural or substantive. Procedural principles address how personal information is collected and used by governing the methods by which data collectors and data providers interact. These principles ensure that consumers have notice of, and consent to, an entity's information practices. Substantive principles, by contrast, impose substantive limitations on the collection and use of personal information, regardless of consumer consent, by requiring that only certain information be collected and that such information only be used in certain ways. Most of the principles discussed below are procedural in nature. One substantive principle widely adopted by the fair information practice codes, but not discussed below, is the collection limitation principle, which states that entities should only collect personal information necessary for a legitimate business purpose. *See* Privacy Protection Study at 513-15; IITF Report §II.A; CSA Model Code ¶4.4.
11. ↑ Federal Trade Comm'n, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress 14 (May 2000) (hereinafter "2000 FTC Report").
12. ↑ *See, e.g.,* OECD Guidelines, Explanatory Memorandum ¶52.
13. ↑ While notice of a Web site's policies with respect to data integrity and security is critical to making an informed decision to reveal personal data, such notice is not a prerequisite to the implementation of security measures. The implementation of security measures lies solely in the hands of the entity collecting the information and requires no active participation from the consumer. Implementation of the principles of choice and access, by contrast, require consumer involvement and, therefore, are dependent on notice to be meaningful.
14. ↑ OECD Guidelines, Openness Principle & ¶12; EU Directive art. 10; CSA Model Code ¶4.8.2.
15. ↑ HEW Report at 62; Privacy Protection Study at 514; OECD Guidelines, Purpose Specification Principle & ¶9; IITF Report §II.B.; Commerce Report at 21; EU Directive art. 10; CSA Model Code ¶4.2. The corollary to identifying the purposes for data collection is that the data not be used for other purposes without the data subject's consent. *See* HEW Report at 61-62; OECD Guidelines, Use Limitation Principle & ¶10 and Explanatory Memorandum ¶55; IITF Report §II.D; EU Directive arts. 6-7; CSA Model Code ¶4.5.
16. ↑ EU Directive art. 10.
17. ↑ Commerce Report at 21.
18. ↑ HEW Report at 59; IITF Report §II.B; EU Directive art. 10. Several of the fair information practice codes recognize that a consumer's refusal to allow the further unrelated use of his or her personal information, beyond that which is necessary to complete the transaction at issue, should not form the basis for the denial of access to the good or service in question. *See, e.g.,* Commerce Report at 25; CSA Model Code ¶4.3.3.

19. ↑ Privacy Protection Study at 514; IITF Report §II.B. Notice of this type is not a prerequisite to insuring the confidentiality, integrity, and quality of data. However, when dealing with data considered by consumers to be particularly sensitive, information about the steps taken by the data collector is important to the consumer and may determine whether the consumer is willing to provide such data.
20. ↑ HEW Report at 58; CSA Model Code ¶ 4.8.2; EU Directive art. 10.
21. ↑ HEW Report at 58; EU Directive art. 10.
22. ↑ IITF Report §II.B.
23. ↑ *Cf.* CSA Model Code ¶4.8.2 (organizations should make available identity of individual accountable for organization's policies and to whom complaints can be forwarded).
24. ↑ HEW Report at 41, 61; OECD Guidelines, Collection Limitation Principle & ¶7 and Use Limitation Principle & ¶10; Commerce Report at 23-27; EU Directive arts. 7, 14; CSA Model Code, ¶¶ 4.3, 4.5; *see also* FTC Report to Congress: Individual Reference Services (Dec. 1997)[1] at 22-23 [hereinafter "FTC Report to Congress/Reference Services"].
25. ↑ 2000 FTC Report, at 15.
26. ↑ *See* Commerce Report at 24-27 (proposing opt-in regimes for "sensitive information" and opt-out regimes for other information).
27. ↑ Indeed, technological innovations soon may allow consumers and collectors of information to engage in "electronic negotiation" regarding the scope of information disclosure and use. Such "negotiation" would be based on electronic matching of pre-programmed consumer preferences with websites' information practices. The World Wide Web Consortium ("W3C") has developed its Platform for Privacy Preferences Project ("P3P")[2], which allows implementation of such technology.
28. ↑ A system requiring consumers to specify privacy preferences before visiting a website can be built into Internet browsers. The absence of default rules, and the concomitant requirement that consumers decide how they want their personal information used, help ensure that consumers in fact exercise choice.
29. ↑ *See* HEW Report at 41, 59, 63; Privacy Protection Study at 508-13; OECD Guidelines, Individual Participation Principle & ¶13; IITF Report §III.B; EU Directive art. 12; CSA Model Code ¶4.9; FTC Report to Congress/Reference Services at 21-22. *See also* Fair Credit Reporting Act ("FCRA") §§609-11, 15 U.S.C. §§1681g-1681i (providing for consumer access to, and the right to correct inaccuracies in, consumer credit reports).
30. ↑ *See* HEW Report at 63; IITF Report §III.B; CSA Model Code ¶4.9; OECD Guidelines, Individual Participation Principle & ¶13 and Explanatory Memorandum ¶61; EU Directive art. 12; *see also* FTC Report to Congress/Reference Services at 21-22; FCRA §611, 15 U.S.C. §1681i.
31. ↑ HEW Report at 56-57; Privacy Protection Study at 521; OECD Guidelines, Data Quality Principle & ¶8 and Explanatory Memorandum ¶53; IITF Report §I.C; EU Directive art. 6; CSA Model Code ¶¶ 4.5.3, 4.6; *see also* FCRA § §605, 607(b), 15 U.S.C. § §1681c, 1681e(b).
32. ↑ OECD Guidelines, Security Safeguards Principle & ¶11 and Explanatory Memorandum ¶56; IITF Report § §I.B, II.C; EU Directive art. 17; CSA Model Code ¶4.7. Physical security measures, such as guards, alarms, etc., may also be necessary in certain circumstances.
33. ↑ In implementing security measures, companies should be aware that security breaches directed at stored data — *i.e.,* information already received by the data collector — often constitute greater threats to privacy than those breaches occurring during the transmission of sensitive data, such as credit card numbers, over the Internet.
34. ↑ *See* HEW Report at 50 (calling for Code of Fair Information Practices that includes civil and criminal penalties, the availability of injunctive relief, and individual rights of action for actual, liquidated, and punitive damages); OECD Guidelines, Accountability Principle & ¶14 and Explanatory Memorandum ¶62 (accountability supported by legal sanctions); IITF Report §III.C ("envision[ing] various forms [of redress] including . . . informal complaint resolution, mediation, arbitration, civil litigation . . . ."); EU Directive arts. 22-23 (judicial remedy and compensation).
35. ↑ Cf. Privacy Protection Study at 33 (identifying voluntary compliance, statutorily-created rights enforceable through individual or government action, and centralized government mechanisms as means of implementing compliance).
36. ↑ The European Union ("EU") has recognized that self-regulation may in certain circumstances constitute "adequate" privacy protection for purposes of the EU Directive's ban on data transfer to countries lacking "adequate" safeguards. *See* EU Directive art. 25. The EU has noted, however, that non-legal rules such as industry association guidelines are relevant to the "adequacy" determination only to the extent they are complied with and that compliance levels, in turn, are directly related to the availability of sanctions and/or external verification of compliance. *See* European Commission, Directorate General XV, Working Document: Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country? (1998) [hereinafter "Judging Industry Self-Regulation"][3].
37. ↑ Discussion Draft: Elements of Effective Self-Regulation for Protection of Privacy (1998) [hereinafter "Elements of Effective Self-Regulation"][4] (identifying consumer recourse, verification, and consequences as elements of an effective self-regulatory regime).

38. ↑ *Id.* In 1997 the Direct Marketing Association ("DMA") asked the FTC for an advisory opinion concerning whether the antitrust laws would permit it to require three things of its members: (1) to use the DMA's Mail Preference and Telephone Preference Services to honor consumers' requests to not be contacted by direct marketers; (2) to disclose to consumers how members sell or otherwise transfer personal information about those consumers to others; and (3) to honor consumers' requests that the members not sell or transfer their personal information. The FTC Bureau of Competition staff advised the DMA of its conclusion that these requirements, as the DMA described them, would not harm competition or violate the FTC Act. *See* Letter from Bureau of Competition Assistant Director to Counsel for the DMA, Sept. 9, 1997 (full-text).
39. ↑ *See* Elements of Effective Self-Regulation.
40. ↑ FTC Report to Congress/Reference Services at 25-33. It is still too early to assess the success or efficacy of this plan, because its provisions are not mandatory on its signatories until the end of the year.
41. ↑ There may, alternatively, be a role for mechanisms to address practices affecting consumers as a group, such as industry or trade association ethics or screening committees that can resolve broader disputes.
42. ↑ *See* Elements of Effective Self-Regulation.
43. ↑ Several fair information practice codes suggest compensation for injuries as an important element of fair information practice. *See* HEW Report at 50 (calling for Code of Fair Information Practices that provides for actual, liquidated, and punitive damages); OECD Guidelines, Accountability Principle & ¶14 and Explanatory Memorandum ¶62 (accountability supported by legal sanctions); IITF Report §III.C ("envision[ing] various forms [of redress] including . . . informal complaint resolution, mediation, arbitration, civil litigation . . . ."); see also Judging Industry Self-Regulation at 5.
44. ↑ HEW Report at 50 (calling for Code of Fair Information Practices that includes civil and criminal penalties, the availability of injunctive relief, and individual rights of action for actual, liquidated, and punitive damages); OECD Guidelines, Accountability Principle & ¶14 and Explanatory Memorandum ¶62 (accountability supported by legal sanctions); IITF Report §III.C ("envision[ing] various forms [of redress] including . . . informal complaint resolution, mediation, arbitration, civil litigation . . . ."); EU Directive arts. 22-23 (judicial remedy and compensation).
45. ↑ Two sectoral privacy acts provide for the recovery of actual, liquidated, and punitive damages for violations. *See* Video Privacy Protection Act of 1988, 18 U.S.C. §2710(c) (providing for award of actual damages or liquidated damages of not less than $2,500, punitive damages, attorney's fees, and equitable relief); Cable Communications Policy Act of 1984, 47 U.S.C. §551(f) (providing for recovery of actual damages or liquidated damages of not less than $1,000, punitive damages, and attorney's fees).
46. ↑ HEW Report at 50; IITF Report §III.C (discussing regulatory enforcement and criminal prosecution as redress options); OECD Guidelines, Explanatory Memorandum ¶62 (referring to accountability supported by legal sanctions); EU Directive art. 24 (unspecified sanctions for violations of directive); see also CSA Model Code ¶4.10.3 (discussing regulatory bodies receiving complaints of violations of fair information practice).
47. ↑ ITF Report §III.C (redress should be appropriate to violation).