

FAIR INFORMATION PRACTICES: A Basic History

Robert Gellman, Privacy and Information Policy Consultant
bob@bobgellman.com

Version 1.6, December 31, 2008

<http://bobgellman.com/rg-docs/rg-FIPshistory.pdf>

Summary

Fair Information Practices (FIPs) are a set of internationally recognized practices for addressing the privacy of information about individuals. Information privacy is a subset of privacy. Fair Information Practices are important because they provide the underlying policy for many national laws addressing privacy and data protection matters.

The international policy convergence around FIPs as core elements for information privacy has remained in place since the late 1970s. Privacy laws in the United States, which are much less comprehensive in scope than laws in some other countries, often reflect some elements of FIPs but not as consistently as the laws of other nations.

Origins of FIPs

Fair Information Practices were initially proposed and named by a U.S. government advisory committee in a 1973 report. The report, *Records, Computers and the Rights of Citizens*,¹ was issued by the Secretary's Advisory Committee on Automated Personal Data Systems. Elliot Richardson, Secretary of the Department of Health, Education and Welfare, established the committee in response to growing use of automated data systems containing information about individuals. The Committee's charge included automated data systems containing information about individuals maintained by both public and private sector organizations.

The chairman of the advisory committee was Willis H. Ware from The Rand Corporation in California. Ware remained an influential expert on privacy matters in following decades. He also served as Vice Chairman of the Privacy Protection Study Commission, a temporary study commission established in the United States by law in 1974.

The central contribution of the Advisory Committee was the development of a code of fair information practices for automated personal data systems. According to Ware, the name *Code of Fair Information Practices* was inspired by the Code of Fair Labor Practices.²

The Committee's original formulation of the Code was:

¹ <http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

² Willis Ware, Addendum A, *A Historical Note* at page 50 in *Health Records: Social Needs and Personal Privacy* (1993) (Conference Proceedings) (Task Force on Privacy, Office of the Assistant Secretary for Planning and Evaluation and the Agency for Health Care Policy and Research, U.S. Department of Health and Human Services), <http://aspe.hhs.gov/pic/reports/ahrq/4441.pdf>.

Safeguards for personal privacy based on our concept of mutuality in record keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice.

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about himself.
- 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 reasonable precautions to prevent misuse of the data.

At approximately the same time the HEW Advisory Committee was established, a similar study about privacy and computers was already underway in Great Britain. A Committee on Privacy chaired by the Rt. Hon. Kenneth Younger was restricted in its terms of reference to private and not public organizations that might threaten privacy.³ To address the potential threats to privacy posed by computerized data, the Younger Committee recommended specific safeguards for automated personal data systems. The main features of the safeguards are:

1. Information should be regarded as held for a specific purpose and not to be used, without appropriate authorization, for other purposes.
2. Access to information should be confined to those authorized to have it for the purpose for which it was supplied.
3. The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose.
4. In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.

³ Great Britain, Home Office, *Report of the Committee on Privacy* (1972) (Rt. Hon. Kenneth Younger, Chairman). This report is not available online. See Appendix B of the 1973 HEW Report for a brief review of the Younger Committee report. <http://aspe.os.dhhs.gov/datacncl/1973privacy/appenb.htm>.

5. There should be arrangements whereby the subject could be told about the information held concerning him.

6. The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.

7. A monitoring system should be provided to facilitate the detection of any violation of the security system.

8. In the design of information systems, periods should be specified beyond which the information should not be retained.

9. Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.

10. Care should be taken in coding value judgments.

The Younger Committee's safeguards contain many of the same elements as the Code of Fair Information Practices proposed by the HEW Advisory Committee. According to one scholar, it is impossible to judge how one committee may have influenced the other.⁴

The Privacy Protection Study Commission (PPSC) also may have contributed to the development of FIPs principles in its 1977 report, Protecting Privacy in an Information Society.⁵ In chapter 13 on the Privacy Act of 1974, the PPSC credited the work of the Congress in refining the five HEW principles into eight during the drafting of the Privacy Act of 1974. The PPSC stated expressly that its identification of the eight principles was the result of the Commission's analysis of congressional actions and was not derived from a specific congressional statement.⁶

These five principles and the findings of the DHEW Committee, published in July 1973, are generally credited with supplying the intellectual framework for the Privacy Act of 1974, though in drafting the statute the Congress, influenced by its own inquiries, refined the five principles to eight.

1. There shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices, and systems. (The Openness Principle)

⁴ Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States at 99 (1992).

⁵ The Commission's report was published by the Government Printing Office. Most of the report can be found online at <http://aspe.hhs.gov/datacncl/1977privacy/toc.htm>.

⁶ PPSC Report at 501, n.5.

2. An individual about whom information is maintained by a record-keeping organization in individually identifiable form shall have a right to see and copy that information. (The Individual Access Principle)

3. An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information. (The Individual Participation Principle)

4. There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information. (The Collection Limitation Principle)

5. There shall be limits on the internal uses of information about an individual within a record-keeping organization. (The Use Limitation Principle)

6. There shall be limits on the external disclosures of information about an individual a record-keeping organization may make. (The Disclosure Limitation Principle)

7. A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate. (The Information Management Principle)

8. A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems. (The Accountability Principle)⁷

The structure of the PPSC version closely resembles the later restatement by the Organization for Economic Cooperation and Development. The OECD version of FIPs has some differences from the PPSC version, including renaming of one principle, reorganizing several principles, and some mild substantive revisions.

Evolution of FIPs

In the 1970s, European nations began to enact privacy laws applicable to the public and private sectors, beginning with Sweden (1973), the Federal Republic of Germany (1977), and France (1978). These laws were consistent with FIPs. Even laws that predated FIPs – including the 1970 Hesse (Germany) law and the 1970 American Fair Credit Reporting Act – reflect the main elements of FIPs.

⁷ PPSC Report at 501-502 (footnote omitted), <http://aspe.hhs.gov/datacncl/1977privacy/c13.htm>. Note that the language that appears on the website of the Department of Health and Human Services Data Council contains a typographical error. A wayward carriage return in the middle of principle 2 produced an apparent nine principles, but the printed report shows eight principles, and there are eight named principles.

As privacy laws spread to other countries in Europe, international institutions took up privacy with a focus on the international implications of privacy regulation. In 1980, the Council of Europe adopted a *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*.⁸ The Convention stated that “it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing.”

The basic principles for data protection in the Council of Europe Convention addressed quality of data, special categories of data, and data security. A data subject should have the right to establish the existence and main purposes of an automated personal data file; the right to confirm whether personal data relating to the data subject are stored in the file; the right to see the data and to rectify or erase the data; and the right to have a remedy for failure to comply with other rights.

The Organization for Economic Cooperation and Development (OECD) proposed similar privacy guidelines around the same time. The *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23 September 1980.⁹

The eight principles set out by the OECD are:

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

⁸ Council of Europe, European Treaty Series No. 108, http://www.privacy.org/pi/intl_orgs/coe/dp_convention_108.txt.

⁹ http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures, which give effect to the principles stated above.

Both the Council of Europe Convention and the OECD Guidelines relied on FIPs as core principles, although neither document used the term. Both organizations revised and extended the original U.S. statement of FIPs, with the OECD Privacy Guidelines being the version most often cited in subsequent years.

As with other versions of FIPs, the OECD Guidelines generally proposes rights and remedies for data subjects while assigning responsibilities to record keepers. The OECD, Council of Europe, and the European Union expressly recognized that disparities in national privacy legislation might create obstacles to the free flow of information between countries. Harmonizing national privacy standards was a major purpose of privacy activities by international organizations, along

with the protection of individual privacy interests. The goal of harmonization helped to raise interest in privacy among the business community.

Statutory Implementation

The HEW Advisory Committee's recommendation for a federal privacy statute resulted in the first statutory implementation of FIPs. The Privacy Act of 1974¹⁰ applies FIPs to federal agencies in the United States. However, it was not until 2002 that the U.S. Congress first formally referenced FIPs in a statute. In establishing a privacy office at the Department of Homeland Security, the Congress assigned the office responsibility for assuring compliance with fair information practices as set out in the Privacy Act of 1974.¹¹

Around the same time that the U.S. enacted the Privacy Act of 1974, European countries began to pass national privacy laws applicable to the public and private sectors. The policies contained in FIPs formed the basis for most national laws. Pressure grew in Europe for more uniformity in privacy law.

In 1995, the EU adopted Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.¹² The reliance on FIPs by the European Union in its data protection directive ensured the spread of FIPs throughout Europe.

The Directive restricted the export of personal information to third countries that did not ensure an "adequate level of protection". This encouraged some other countries to conform their laws to the FIPs principles that formed the basis of the directive. National laws found by the EU to be adequate are available at an EU Data Protection webpage.¹³

Canada took a different procedural approach in the early 1990s when it sought to establish a privacy *standard*. The Canadian Standards Association (CSA) led the Canadian privacy effort. Representatives of all stakeholders, including government, business, and consumer interests participated in the process. CSA published the Model Code as a National Standard of Canada in 1996.¹⁴ The CSA standard follows the international consensus on FIPs. The CSA standard has ten interrelated principles that can be readily mapped to the OECD Guidelines. In 2000, Canada enacted the standard directly into law as the basis for its private sector privacy legislation.¹⁵

¹⁰ 5 U.S.C. §552a. The findings and the purposes of the original Act – Public Law 93-579 – reflect the influence of the HEW Advisory Committee, and the substantive provisions of the Act also were derived largely from the Committee's report.

¹¹ 6 U.S.C. §142. Similar FIPs language can be found in 50 U.S.C. § 403-3d(b)(5) (establishing a Civil Liberties Protection Officer within the Office of the Director of National Intelligence).

¹² http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

¹³ http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

¹⁴ <http://www.csa.ca/standards/privacy/code/Default.asp?language=english>.

¹⁵ Personal Information Protection and Electronic Documents Act, http://www.privcom.gc.ca/legislation/02_06_01_e.asp.

Comment and Criticism

While there is broad international agreement on the substance of FIPs, different statements of FIPs sometimes look different. Further, statutory implementations of FIPs may vary in different countries, contexts, and sectors. There can be multiple ways to comply with FIPs for different types of records and record keepers.

In the United States, elements of FIPs are occasionally required by law for specific classes of record keepers or categories of records. Otherwise, private sector compliance with FIPs principles, while slowly increasing, is mostly voluntary and sporadic. Also, shortened or incomplete versions of FIPs have sometimes been offered in the United States by federal agencies or trade associations. *Notice and choice* is sometimes presented as an implementation of FIPs, but it typically falls well short of FIPs standards.

Other incomplete versions of FIPs can also be found. In 2000, the Federal Trade Commission recommended that commercial websites that collect personal identifying information from or about consumers online should be required to comply with “the four widely-accepted fair information practices.” The FTC’s version of FIPs includes only notice, choice, access and correction, and security. The FTC’s set of privacy standards restates, waters down, and leaves out some FIPs elements.¹⁶

The FTC’s 2000 version of FIPs is shorter and less complete than a version issued by the Privacy Office at the Department of Homeland Security in 2008. The DHS version, called Fair Information Practice Principles, includes eight principles that match up closely with the OECD version.¹⁷ The DHS issuance is noteworthy since it implements the first statutory reference to fair information practices.

FIPs are not self-implementing or self-enforcing. Actual implementation of FIPs at the statutory, regulatory, or data controller level can vary widely, depending on the country, the data controller, the type of data, other conflicting goals, and other factors. For example, accountability can be met through many different mechanisms, including criminal or civil penalties; national or provincial supervisory officials; other administrative enforcement; various forms of self-regulation including industry codes and privacy seals; formal privacy policies; compliance audits; employee training; privacy officers at the data controller level; and other methods. Similarly, providing data subjects with access to their own records may have different exceptions, depending on whether the records are maintained for employment, educational, credit, or law enforcement purposes.

Critics of FIPs can be found on both sides. Some in the privacy community believe that FIPs are too weak, allow too many exemptions, do not require a privacy agency, fail to account for the

¹⁶ Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace, (May 2000), <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

¹⁷ See Department of Homeland Security, Privacy Policy Guidance Memorandum (2008) (Memorandum Number 2008-1), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

weaknesses of self-regulation, and have not kept pace with information technology.¹⁸ Critics from a business perspective often prefer to limit FIPs to reduced elements of notice, consent, and accountability. They complain that other elements are unworkable, expensive, or inconsistent with openness or free speech principles.

In 1999, Mr. Justice Michael Kirby of the High Court of Australia and former chair of the OECD Committee that developed the 1980 Guidelines spoke at an international privacy conference. He noted the many changes brought about by new computer and communication technologies and suggested that it may be time for a review of the guidelines. Among new rights that he mentioned as ripe for review were:

1. A right not to be indexed.
2. A right to encrypt personal information effectively.
3. A right to fair treatment in key public infrastructures so that no person is unfairly excluded in a way that would prejudice that person's ability to protect their privacy.
4. A right to human checking of adverse automated decisions and a right to understand such decisions.
5. A right, going beyond the aspiration of the 'openness principle', of disclosure of the collections to which others will have access and which might affect the projection of the profile of the individual concerned.¹⁹

No formal attempt to restate FIPs has been undertaken in recent years.

Version History

Version 1.5 adds a discussion about the restatement of FIPs in the report of the Privacy Protection Study Commission. (September 2008). Thanks to Marc Rotenberg for pointing out the PPSC's connection to FIPs.

Version 1.6 adds a paragraph about the Department of Homeland Security's 2009 version of FIPs. It also adds a footnote reference to FIPs language in the statute establishing a Civil Liberties Protection Officer within the Office of the Director of National Intelligence.

¹⁸ Roger Clarke has been a leading critic of FIPs. See, e.g., his paper on *Research Use of Personal Data*, <http://www.anu.edu.au/people/Roger.Clarke/DV/NSCF02.html>.

¹⁹ Michael Kirby, *Privacy Protection – A New Beginning*, (1999) (speech before the 21st International Conference on Privacy and Personal Data Protection), <http://www.pco.org.hk/english/infocentre/conference.html>.