**ROBERT GELLMAN**
**Privacy and Information Policy Consultant** **202-543-7923**
**419 Fifth Street SE** **bob@bobgellman.com**
**Washington, DC 20003** **www.bobgellman.com**

# FAIR INFORMATION PRACTICES: A Basic History

**Robert Gellman**[G]

**Version 2.22, April 6, 2022**


I maintain this document at https://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf. You can also find it at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020. Send suggestions for changes and updates to bob@bobgellman.com.

## Summary

This report offers a history of **Fair Information Practices** (FIPs) with a focus – but not an exclusive one – on activities in the United States. The text usually quotes key portions of source documents in order to allow for comparison of different versions of FIPs. For the most part, the analysis is neutral, with only limited interpretation, comment, and criticism.

**FIPs are a set of internationally recognized practices for addressing the privacy of information about individuals. Information privacy is a subset of privacy.** FIPs 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 most other nations.

**FIPs began in the 1970s with a report from the Department of Health, Education & Welfare. The Organisation for Economic Cooperation and Development revised the principles in a document that became influential internationally.** FIPs have evolved over time, with different formulations coming from different countries and different sources over the decades. A 2013 revision by the Organisation for Economic Cooperation and Development retained the original statement of privacy principles. Elements in addition to FIPs are increasingly recognized today as part of international privacy policy discussions, standards, and laws. Many today consider FIPs to be necessary but not sufficient as privacy standards.

---

[*] Privacy and Information Policy Consultant, Washington, DC; former Chief Counsel and Staff Director, Subcommittee on Government Information, Committee on Government Operations, U.S. House of Representatives; J.D. 1973, Yale Law School. https://www.bobgellman.com.

# Table of Contents

I. Origins of FIPs ..... 3
II. Evolution of FIPs ..... 9
A. Origins and Early History ..... 9
B. Recent History ..... 13
III. Statutory and Other Implementations of FIPs ..... 14
A. U.S., EU Data Protection Directive, and the General Data Protection Regulation ..... 14
B. Canada ..... 16
IV. More U.S. Versions of FIPs ..... 23
A. 1998 & 2000 FTC ..... 24
B. 2008 DHS ..... 25
C. 2011 NSTIC ..... 27
D. 2011 National Science and Technology Council ..... 28
E. 2012 Department of Commerce ..... 29
F. 2012 FTC ..... 32
G. 2012 HHS ONC Principles ..... 34
H. 2013 Executive Order on Improving Critical Infrastructure Cybersecurity ..... 42
I. OMB Guidance for Providing and Using Administrative Data for Statistical Purposes ..... 42
J. Obama White House Big Data Report ..... 42
K. OMB Circular A-130 ..... 43
L. NIST Privacy Engineering and Risk Management in Federal Systems ..... 45
M. Energy Act of 2020 ..... 45
V. Comment and Criticism about FIPs ..... 46
Appendix 1: Modernizing the 1980 OECD Statement of FIPs ..... 54
Version History for this Document ..... 57

# I. Origins of FIPs

In a 1973 report, a U.S. government advisory committee initially proposed and named Fair Information Practices as a set of principles for protecting the privacy of personal data in record-keeping systems. The Secretary's Advisory Committee on Automated Personal Data Systems issued the report, *Records, Computers and the Rights of Citizens*.[1] 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 later served as Vice Chairman of the Privacy Protection Study Commission, a temporary study commission established in the United States by law in 1974.[2]

The central contribution of the Advisory Committee was the development of a code of fair information practices for automated personal data systems.[3] According to Ware, the name *Code of Fair Information Practices* was inspired by the Code of Fair Labor Practices.[4] Carole Parsons

---

[1] http://epic.org/privacy/hew1973report/default.html.

[2] Pub. L. 93–579, §5, Dec. 31, 1974, 88 Stat. 1905. See also Pub. L. 95-38, June 1, 1977, 91 Stat. 179 (extending the life of the PPSC until Sept. 30, 1977).

[3] It has often been said that reports by commissions and advisory committee end up *gathering dust on a shelf*, meaning that they are ignored. The HEW Advisory Committee was, perhaps, one of the most influential reports of its type, with long-lasting international effects that continue more than forty years later. See Robert Gellman, *Willis Ware's Lasting Contribution to Privacy: Fair Information Practices*, 12 IEEE Security & Privacy 51 (2014), http://doi.ieeecomputersociety.org/10.1109/MSP.2014.82. See also Deirdre K. Mulligan, *The Enduring Importance of Transparency*, 12 IEEE Security & Privacy 61(2014), http://doi.ieeecomputersociety.org/10.1109/MSP.2014.58; K Evans, *Where in the World Is My Information?: Giving People Access to Their Data*, 12 IEEE Security & Privacy 78(2014), http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6924618#.

[4] 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), https://aspe.hhs.gov/pdf-report/health-records-social-needs-and-persona-privacy. The name of this document on the HHS website has a typo (*persona* rather than *personal*), as does the link.
The story also appears in Willis H. Ware, RAND AND THE INFORMATION EVOLUTION A History in Essays and Vignettes at 157 (2008) (RAND), http://www.rand.org/content/dam/rand/pubs/corporate_pubs/2008/RAND_CP537.pdf. I reproduce the key paragraphs here (footnotes omitted) in case the book disappears from the web.

> The Origin of the Phrase 'Code of Fair Information Practices'
>
> The following reconstruction of history is based on my recollections of the time, an interchange of electronic-mail messages with John Fanning [presently with the U.S. Public Health Service, Commissioned Corps, or USPHS], and correspondence with David B. H. Martin, Executive Director of the [HEW] Secretary's Advisory Committee on Automated Personal Data Systems [SACAPDS]. The associate executive director of SACAPDS was Carole Watts Parsons, now Mrs. William Bailey.
> The so-called "HEW committee," assembled and tasked by [then HEW] Secretary Elliot Richardson, had often met in Bethesda, Maryland and held meetings at the local Holiday Inn.

Occasionally we would also use the NIH facilities at Bethesda for a meeting. The agenda would normally call for a 3-day meeting and on at least two occasions, a Saturday was included.
On a particular occasion, we had met on a Saturday in one of the NIH buildings. It was out-of-hours for the building and the security guard required us to sign in individually and also to give our SSNs. There was a lot of joking among committee members about this because we had been discussing the SSN in committee and regarded this activity by NIH as completely inappropriate. It was in winter because everyone had street coats.
There had been a discussion on Friday night between me and David Martin in which he outlined the concept of adopting a set of rules that would be the basis for the relationship between a data subject and a record keeper. On Saturday morning, I made a presentation about the concept of a list of standard practices as a way of dealing with privacy issues and I also presented arguments supporting it as a reasonable and sensible approach. In discussing it, the committee undertook to construct a list of what features might be on such a list.
As we thought of them, Professor Layman Allen from the University of Michigan Law School and member of the committee wrote them on a board at the end of the meeting room. I remember that initially, there were only a few entries on the list. Computer-oriented people in the group of course thought of all manner of rules to [ensure] accuracy, correction of errors, etc.
One such proposal was to require the record keeper to notify all who had received personal information from it of the correction. We quickly estimated that it would be a back breaking task for the record keeper, and that it would be a superb source of income for the U.S. Postal Service.
David Martin and I departed the meeting for some outside obligation. We left Layman Allen in charge and when we came back an hour or so later, the group had expanded the list to [I think] about a dozen items. By that time, it was midafternoon and we adjourned the meeting and went home. David and I exchanged some private comments as we left that the list of rules had become very complex; we were both a little dismayed at what had happened.
The committee report . . . lists the dates of the meetings but not the places. Comparing them to calendars for 1972 and 1973, and given that the time of year was winterish, the meeting in question could have been December 16, 1972 [Saturday] or March 3, 1973 [Saturday].
The December date is more likely to have been “winterish” and had only one speaker scheduled whereas the March date seems too late, given that the agenda for it is shown as “discussion of the final report.” Keep in mind that the final report printed by the U.S. Government Printing O ce was presented to [then] Secretary Caspar Weinberger in June, 1973. Thus, December 16, 1972 appears to be the day on which the committee framed the essence of a Fair Code, but did not name it.
The dates of March 1–3, 1973 are shown to be the 7th and final meeting of the committee, and we would certainly have had the details of the “list of rules” and its name settled by then. While there were no formal committee meetings between December 1972 and March 1973, there were additional drafting meetings, and draft review meetings among David Martin, Carole Parsons and myself.
In the December–March interval not only did a full draft of the report get created but the lengthy list of features from December got boiled down to its present size. I believe that this was primarily the work of David Martin and Carole Parsons, probably in discussion with me either by phone or in a review meeting in Washington. I do recall that David and I often had very lengthy phone conversations. We also worked out an arrangement for exchanging draft materials and comments between Washington and Santa Monica on an overnight basis. The December– March period was an intensive one of writing and re-writing.
After such a drafting/review meeting, David, Carole, and I were sitting around a table in the north building of the old HEW complex, probably on the 5th floor which was where the o ces of the committee were. It would have been around dinner time and other people, mostly friends of David, drifted in and out. We were winding down after the day and chatting about various details of the report.
Someone came into the room, was introduced to me, and [I believe] was also characterized as having worked with or was presently with the Department of Labor. The 3 of us had been talking about our list of protective mechanisms and I suspect toying with names for it.

Bailey, Associate Executive Director of the HEW advisory committee confirmed parts of Ware's recollection.[5]

The Committee's original formulation of the Code was:

> 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.

---

> The individual who had drifted in mused out loud to the e ect: "What we're talking about is just like the Code of Fair Labor Practices." That was a pivotal comment and promptly, David Martin first voiced the phrase "Code of Fair Information Practices." I believe we might have bandied about variations on the phrase—such as where to put the word "fair"—but one struck us as best and has survived.
> The identity of the individual who commented about the similarity to the Fair Labor Practices is uncertain. There is a possibility that it was John Fanning, presently with USPHS. He believes it was not he, so for the moment, the person's identity is unknown.
> It is clear however that David Martin did coin the phrase "Code of Fair Information Practices" and that it occurred in the period between December, 1972 and March 1973. Since the December event was only a week before Christmas, and drafting really got started in January, it is likely that the actual date is in February or the first part of March 1973.
> Slightly ahead of the [HEW] committee was the work of the Younger [Committee on Privacy] in the UK. There were also study groups in several other countries; there are brief summaries of reports and activities in the report about Sweden, France, Germany, Canada, and the UK.
> With respect to the Younger committee specifically, pp 173–174 of the report [summarize] its work and [list] ten "safeguards" [that] bear some resemblance to a Fair Code, but are much less specific and not as crisply stated as the provisions of the Fair Code. The British Computer Society had also adopted a Code of Ethics for its people and the Younger report supported and adopted it also. There is no mention of the term "Fair Code" or even of a "Code" in the summary of the Younger report. In fact, we used its own phrase "safeguards." Had the Younger group used the phrase "Fair Code" or even "Code," I feel certain that we certainly would have acknowledged it and also used it in what we wrote.
> Thus, "Code of Fair Information Practices" appears to be uniquely American and to have been originated by David B. H. Martin.

In personal conversations with the author of this history, John Fanning said he does not believe that he coined the phrase *fair information practices*.

[5] "Unfortunately, I too don't remember offhand who the knowledgeable about Fair Labor Practices was, although I agree that it was not John Fanning. My recollection is that after that encounter in the office, David [Martin], Willis [Ware] and I went to dinner at a long since departed restaurant [Market Inn] in Southwest Washington, not far from our HEW offices. I even remember what I ordered that evening—a salad, bluefish, and a baked potato. If memory serves, we then stood on a corner outside the restaurant continuing to discuss what the term, Fair Information Practices, should reasonably encompass." Email from Carole Parsons Bailey to Robert Gellman (June 24, 2019).

• 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.

In 2014, Professor Chris Hoofnagle from the Berkeley Center for Law and Technology posted transcripts from many of the Secretary's Advisory Committee hearings in 1972.[6] This is a useful resource to those interested in the origins of FIPs. Hoofnagle also provided summaries of the meetings. The transcripts and the summaries are a major contribution to the history of privacy.

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.[7] To address the potential threats to privacy posed by computerized data, the Younger Committee recommended "basic principles" for handling personal data that should apply to the handling of personal information by computers.[8] The principles 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.

---

[6] https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/archive-of-the-meetings-of-the-secretarys-advisory-committee-on-automated-personal-data-systems-sacapds/. See also Chris Jay Hoofnagle, *The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)* (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466418.

[7] 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://epic.org/privacy/hew1973report/appenb.htm. The official copy of the Younger Committee report is available at the British National Archives, but the report is not available in a digital format. http://discovery.nationalarchives.gov.uk/details/r/C11027826?descriptiontype=Full.
Parliamentary discussions about the Younger Committee report in the House of Lords can be found at 343 Parl. Deb., H.L. 104-78 (June 6, 1973), https://api.parliament.uk/historic-hansard/lords/1973/jun/06/privacy-younger-committees-report, and 859 Parl. Deb., H.C. 1955-2058 (July 13, 1973), https://api.parliament.uk/historic-hansard/commons/1973/jul/13/privacy-younger-report.

[8] Younger Committee Report at para. 591. In the same paragraph, the report "acknowledg[es] our debt to those who have adopted or advocated all of some of [the basic principles] and who urge the adoption of a similar code throughout both the public and private sectors."

4. In computerised 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.

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.[9]

The Younger Committee's safeguards contain many of the same elements as the Code of Fair Information Practices proposed by the HEW Advisory Committee.[10] According to one privacy

[9] Younger Committee Report at paras. 592-600.

[10] Some paragraphs from the *Computers* chapter of the Younger Committee Report are worth reproducing here as they include conclusions and recommendations about the basic principles:

> 619. In considering computers and computerised information stores we are very conscious of the fact that the technology is advancing rapidly and we are not as a Committee expert in this field, although we have been able to call upon experts for guidance and advice. We have set out in paragraphs 592 to 600 principles for handing personal information which seem to us desirable and which we have felt able to formulate without technical expertise. We cannot on the evidence before us conclude that the computer as used in the private sector is at present a threat to privacy, but we recognize that there is a possibility of such a threat becoming a reality in the future.
>
> 620. To meet this situation there is a need, in the first place, for the immediate voluntary adoption by computer users of the principles we have enunciated and, in the second, some means of supervising developments and trends in both the technical and non-technical spheres of computer operation. We do not believe that the time is ripe for the sort of detailed controls advocated in the Bills proposed by Mr Baker and Mr Huckfield, though some scheme of registration, licensing and inspection on these lines may be appropriate at a future date.
>
> 621. We therefor recommend that the Government should legislate to provide itself with machinery for keeping under review the growth in and techniques of gathering personal information and processing it with the help of computers. Such machinery should take the form of an independent body with members drawn from both the computer world and outside. For the sake of convenience we call it here a standing commission and it may be helpful if we say something about what we think it should do.
>
> 622. We envisage that it should collect information about computerised personal information stores: their prevalence, purpose, detail, linkage, commercial use and management. It should review the principles of handling personal information laid down in this chapter to determine their relevance and adequacy in a changing situation and consider the case for giving them legislative force. It could receive complaints about

scholar, it is impossible to judge how one committee may have influenced the other.[11] It is clear, however, that the Younger Committee Report is dated July 1972, and the HEW Report is dated July 1973, and that the HEW Report cites the Younger Committee Report.

The Privacy Protection Study Commission (PPSC) also may have contributed to the development of FIPs principles in its 1977 report, Personal Privacy in an Information Society.[12] In chapter 13 on the Privacy Act of 1974, the PPSC said that "the five principles from the HEW Advisory Committee are generally credited with supplying the intellectual framework for the Privacy Act of 1974, thought in drafting the statute the Congress, influenced by its own inquiries, refined the five principles to eight."[13] as inspiration for the PPSC's refining of the five HEW principles into eight principles. The identification of the eight principles resulted from the PPSC's analysis and not a specific congressional document.[14]

> 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)

---

invasions of privacy by the users of computerised information stores. In light of its findings it should, from time to time, make recommendations as it saw fit for legislative or other controls for safeguarding the handling of personal information in computerised stores.

[11] Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States at 99 (1992). Bennett's book is especially useful for its discussion of how international privacy policy converged about FIPs during the 1970s and 1980s. http://www.cornellpress.cornell.edu/book/?GCOI=80140100026690.

[12] The Government Printing Office published the Commission's report. The Department of Health and Human Services has a partial copy at http://aspe.hhs.gov/report/personal-privacy-information-society. A complete version of the report (with all appendices) is on the Electronic Privacy Information Center at https://epic.org/privacy/ppsc1977report/.

[13] PPSC Report at 501.

[14] PPSC Report at 501, n.5. Carole Parsons Bailey, Executive Director of the PPSC, in an email years later, expanded on the development of FIPs by the PPSC:

> With respect to the PPSC (of which I was Executive Director), I wouldn't say that the Commission "credited" the Congress with expanding the five principles into eight, i.e. adding Principles (4), (5) and (8). In fact, the Commission hotly debated the addition of any legislated restriction on questions that might be asked of an individual, thinking that the conceivable array of situations was just too vast and varied.
>
> My recollection is that Principle (5) was added because hearings held by both the Commission and the Congress unearthed the fact that personal data could be shared with impunity within a record keeping organization, for example, by a bank marketing insurance to its account holders. I don't remember that being a finding of the HEW Report.
>
> The Accountability Principle, Principle (8), in my view, was just a refinement of the recommendation on page 64 in the HEW Report about the state of existing law. Again, the Commission debated what kind of penalties should reasonably be applied to FIP violators. Some Commissioners were concerned lest excessive Government regulation be applied, which is why we rejected giving "date protection" [probably should be "data protection"] authority along European lines to the Federal Trade Commission. The guiding thought at the time was that agencies and companies should be allowed to comply voluntarily, at least for the time being.
>
> Remember that in those days the iPhone and Facebook were still the stuff of science fiction.

Email from Carole Parsons Bailey to Robert Gellman (June 24, 2019).

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)[15]

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.

# II. Evolution of FIPs

## A. Origins and Early History

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

[15] 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.

Hesse (Germany) law and even the 1970 American Fair Credit Reporting Act – reflect the main elements of FIPs.

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*.[16] The Convention stated "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 Convention was the first legally binding international treaty on data protection.

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 Council of Europe maintains a data protection webpage that includes, among other things, information on new signatories to the Convention and reports on the modernization of the Convention.[17] The Ad hoc Committee on data protection approved a modernization proposal in December 2014.[18] The Council adopted a modernized Convention 108 in 2018.[19] A summary by the Council describe the changes in these terms:

> With the modernisation of the 1981 Convention 108, its original principles have been reaffirmed, some have been strengthened and some new safeguards have been laid down: They had to be applied to the new realities of the on-line world while new practices had led to the recognition of new principles in the field. The principles of transparency, proportionality, accountability, data minimisation, privacy by design, etc. are now acknowledged as key elements of the protection mechanism and have been integrated in the modernised instrument.[20]

These changes reflect the evolution of privacy standards over time by adding new principles alongside of the original principles that were "reaffirmed".

---

[16] Council of Europe, European Treaty Series No. 108, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.
[17] https://www.coe.int/en/web/data-protection/convention108/modernised.
[18] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Work Programme of the T-Pd for 2014 and 2015 (2014), http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168069459f.
[19] Convention 108+ Convention for the protection of individuals with regard to the processing of personal data (2018), http://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
[20] Council of Europe, The modernised Convention 108: novelties in a nutshell (2018), http://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8.

The Organisation for Economic Cooperation and Development (OECD) proposed similar privacy guidelines around the same time as the Council of Europe's original 1980 effort. A group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission, developed the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The OECD adopted the recommendation, which became applicable on 23 September 1980.[21]

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.
>
> 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.

---

21 http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

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.

Along with the 1980 Privacy Guidelines, the OECD issued an explanatory memorandum whose purpose was to "explain and elaborate the Guidelines and the basic problems of protection of privacy and individual liberties."[22]

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 proposed rights and remedies for data subjects while assigning responsibilities to record keepers. The OECD, Council of Europe, and the European Union (EU) 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.

[22] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum* at Introduction. The memorandum is accessible at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

## B. Recent History

In 2013, the OECD issued revised guidelines in a document titled *The OECD Privacy Framework*.[23] The foreword to the document noted that, "as compared with the situation 30 years ago, there has been a profound change of scale in terms of the role of personal data in our economies, societies, and daily lives," and that "[t]he environment in which the traditional privacy principles are now implemented has undergone significant changes."[24]

It is noteworthy that the Expert Group that prepared the revisions did not amend the eight basic principles from the 1980 Guidelines. The OECD version of FIPs remained unchanged, while other materials were adjusted and added.

> The Expert Group took the view that the balance reflected in the eight basic principles of Part Two of the 1980 Guidelines remains generally sound and should be maintained. The Expert Group introduced a number of new concepts to the OECD privacy framework, such as privacy management programmes, security breach notification, national privacy strategies, education and awareness, and global interoperability. Other aspects of the 1980 Guidelines were expanded or updated, such as accountability, transborder data flows and privacy enforcement.[25]

It is beyond the scope of this document to fully describe or evaluate how the OECD revised its privacy guidance and accompanying documentation. The 2013 explanatory memorandum takes into account the many changes in international privacy activities, privacy laws, and privacy policy that took place between 1980 and 2013. The OECD placed a greater emphasis on management, transborder data flows, security breach notification, enforcement and management, and international cooperation.

The Australian Privacy Foundation (APF), which represents privacy advocates, found the decision to leave the basic principles from 1980 unchanged to be a "missed opportunity to respond to the developments of the last 35 years." APF found the new part on implementing accountability to be the "only significant positive addition." APF also criticized other changes that appear to restrict "the ability of countries to limit exports of personal information to jurisdictions with weaker privacy standards." In general, APF opposed continuing recognition of the revised OECD Guidelines as an international data privacy standard, but it found the basic principles "continue to play a useful role as a minimum set of data privacy principles which it is valuable for countries to enact if they [have] no data privacy law and it is not possible for them to enact stronger provisions, in preference to no data privacy law at all."[26]

---

[23] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. The document includes a wealth of materials, including the original 1980 guidelines and explanatory materials, a 2013 supplementary explanatory memorandum, and a 2011 OECD paper titled: *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*.
[24] Id at 3.
[25] Id. at 22.
[26] Australian Privacy Foundation, *International Data Privacy Standards: A Global Approach (Australian Privacy Foundation Policy Statement)* at section 2 (17 Sept. 2013), http://www.privacy.org.au/Papers/PS-IntlDP.pdf.

# III. Statutory and Other Implementations of FIPs

## A. U.S., EU Data Protection Directive, and the General Data Protection Regulation

The HEW Advisory Committee's recommendation for a federal privacy statute resulted in the first statutory implementation of FIPs anywhere in the world. The Privacy Act of 1974[27] applies FIPs to federal agencies in the United States. Massachusetts enacted a Fair Information Practices chapter to its general laws in 1975.[28] Minnesota enacted a Minnesota Government Data Practices Act implementing fair information practices in 1974.[29]

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 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."[30]

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.[31] 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.[32]

The text of the 1995 data protection directive fully reflects FIPs principles, albeit with some variation. The provisions that implement FIPs are in various places in the directive.

---

[27] 5 U.S.C. § 552a. http://www.law.cornell.edu/uscode/text/5/552a. The findings and the purposes of the original Act – Public Law 93-579 – reflect the influence of the HEW Advisory Committee. Congress based the substantive provisions of the Act largely on the Committee's report.

[28] Mass. Gen. Laws ch. 66A, https://malegislature.gov/Laws/GeneralLaws/PartI/TitleX/Chapter66A. The Massachusetts law applies to state agencies and contractors a version of FIPs that bears some similarities to the federal Privacy Act of 1974.

[29] Minn. Stat. § 13.01 et seq. https://www.revisor.mn.gov/statutes/?id=13.01. The author of the Act, State Senator Robert Tennessen, was at the time of enactment a member of the Privacy Protection Study Commission.

[30] 6 U.S.C. § 142(a)(2), http://www.law.cornell.edu/uscode/text/6/142. The language was reportedly added to the legislation at my suggestions and the suggestion of several privacy advocates. Other references to FIPs in U.S. Code can be found in a later footnote.

[31] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT.

[32] http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm.

By contrast, the 2016 General Data Protection Directive (GDPR),[33] which has an effective date of May 25, 2018, effectively offers an index to and restatement of most FIPs principles in Article 5 ("*Principles relating to processing of personal data*"). The text of Article 5 is:

> Article 5
>
> Principles relating to processing of personal data
>
> 1. Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

[33] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0011.

> 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Additional articles of the GDPR explain in more detail how data controllers must implement the rights indexed in Article 5.

Article 5 references all FIPs principles except for Individual Participation. Part III of the GDPR on the rights of data subjects addresses the right of access and the right of rectification in Article 15 ("*Right of access by the data subject*") and Article 16 ("*Right to rectification*"). Depending on your perspective, Article 17 ("*Right to erasure ('right to be forgotten')*") is an extension of FIPs principles or an entirely additional right.

## B. Canada

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 1995.[34] The CSA standard follows the international consensus on FIPs. The CSA standard has ten interrelated principles that readily map to the basic principles of the OECD Guidelines. In 2000, Canada enacted the standard directly into law as the basis for the Personal Information Protection and Electronic Documents Act (PIPEDA), the Canadian private sector privacy legislation.[35]

In addition to its enactment into law, the CSA Standard is noteworthy for its nuance and its implementation details. It is much longer than any of the other FIPs versions reproduced in this history. The text of the CSA Standard from PIPEDA is:

> **Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96**
>
> **4.1 Principle 1 — Accountability**
> An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
> 4.1.1. Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

---

[34] The Canadian Standard Association places its codes behind a paywall. The text is available from others without cost. See http://simson.net/ref/RSA/1996.CanadianStandardsAssociation.ModelCodeForProtectionOfPersonalInfo.pdf.

[35] Personal Information Protection and Electronic Documents Act, http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. The CSA code is in Schedule 1 (Section 5) of PIPEDA at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html.

4.1.2. The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.
4.1.3. An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
4.1.4. Organizations shall implement policies and practices to give effect to the principles, including
(a) implementing procedures to protect personal information;
(b) establishing procedures to receive and respond to complaints and inquiries;
(c) training staff and communicating to staff information about the organization's policies and practices; and
(d) developing information to explain the organization's policies and procedures.

**4.2 Principle 2 — Identifying Purposes**
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
4.2.1. The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).
4.2.2. Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.
4.2.3. The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.
4.2.4. When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).
4.2.5. Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.
4.2.6. This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

**4.3 Principle 3 - Consent**
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1. Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2. The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3. An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4. The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5. In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual’s name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual’s request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-

care products, unless consent were obtained. Consent shall not be obtained through deception.
4.3.6. The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).
4.3.7. Individuals can give consent in many ways. For example:
(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
(c) consent may be given orally when information is collected over the telephone; or
(d) consent may be given at the time that individuals use a product or service.
4.3.8. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

**4.4 Principle 4 — Limiting Collection**
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
4.4.1. Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).
4.4.2. The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.
4.4.3. This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

**4.5 Principle 5 —Limiting Use, Disclosure, and Retention**
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

4.5.1. Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).
4.5.2. Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.
4.5.3. Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.
4.5.4. This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

**4.6 Principle 6 — Accuracy**
Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
4.6.1. The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.
4.6.2. An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.
4.6.3. Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

**4.7 Principle 7 — Safeguards**
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
4.7.1. The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.
4.7.2. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.
4.7.3. The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4. Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5. Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

**4.8 Principle 8 — Openness**

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1. Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization’s policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2. The information made available shall include

(a) the name or title, and the address, of the person who is accountable for the organization’s policies and practices and to whom complaints or inquiries can be forwarded;

(b) the means of gaining access to personal information held by the organization;

(c) a description of the type of personal information held by the organization, including a general account of its use;

(d) a copy of any brochures or other information that explain the organization’s policies, standards, or codes; and

(e) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3. An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

**4.9 Principle 9 — Individual Access**

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should

be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1. Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2. An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3. In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4. An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5. When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6. When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

**4.10 Principle 10 — Challenging Compliance**

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

4.10.1. The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

> 4.10.2. Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.
> 4.10.3. Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.
> 4.10.4. An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

The U.S. Department of Health and Human Services relied upon FIPs in issuing a privacy rule under the Health Insurance Portability and Accountability Act (HIPAA). In adopting the rule, HHS said, "This final rule establishes, for the first time, a set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care."[36] The Department referenced but did not restate FIPs principles in the rule itself. The HIPAA privacy rule implements all FIPs principles in some way, but the collection limitation principle is lightly applied, presumably because HHS did not want to tell health care providers what information to collect while treating patients.

## IV. More U.S. Versions of FIPs

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, occasional laws require some elements of FIPs for specific classes of record keepers or categories of records.[37] Otherwise, private sector compliance with FIPs principles,

---

[36] Department of Health and Human Services, Final Rule, *Standards for Privacy of Individually Identifiable Health Information*, 65 Federal Register 82462, 82464 (Dec. 28, 2000) at http://www.gpo.gov/fdsys/pkg/FR-2000-12-28/pdf/00-32678.pdf. See also id. at 82487 ("…our privacy regulation [is] based on common principles of fair information practices.").

[37] There are FIPs references in statute in: 50 U.S.C. § 3029(b)(5), http://www.law.cornell.edu/uscode/text/50/3029, (establishing a Civil Liberties Protection Officer within the Office of the Director of National Intelligence); in 42 U.S.C. § 2000ee-2, http://www.law.cornell.edu/uscode/text/42/2000ee-2, (requiring the Attorney General, the Secretary of Defense, the Secretary of State, the Secretary of the Treasury, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the head of any other department, agency, or element of the executive branch designated by the Privacy and Civil Liberties Oversight Board to have a privacy and civil liberties officer);. in 49 U.S.C. § 31306a(d)(1), establishing a national clearinghouse for controlled substance and alcohol test results of commercial motor vehicle operators that must comply with applicable Federal privacy laws, including the fair information practices under the Privacy Act of 1974, http://www.law.cornell.edu/uscode/text/49/31306a; in the Transportation Security Acquisition Reform Act, Pub. L. 113-245 § 3, 128 Stat. 2871, 6 U.S.C. 563a, (requiring the Administrator of the Transportation Security Administration to determine whether any security-related technology acquisition is

while increasing, is mostly voluntary and sporadic. In addition, shortened or incomplete versions of FIPs have sometimes been offered in the United States by federal agencies or trade associations.[38] *Notice and choice* is sometimes presented as an implementation of FIPs, but it clearly falls well short of FIPs standards. Other incomplete versions of FIPs can also be found.

### A. 1998 & 2000 FTC

In a 1998 report, the Federal Trade Commission identified the "five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress."[39] In 2000, the 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."

> (1) Notice - Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
>
> (2) Choice - Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).
>
> (3) Access - Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.

---

justified by conducting an analysis that includes, among other things, a determination that the proposed acquisition is consistent with fair information practice principles issued by the Privacy Officer of the Department, https://www.law.cornell.edu/uscode/text/6/563a;The Cybersecurity Act of 2015, Pub. L. 114–113, div. N, title I, § 105, Dec. 18, 2015, 129 Stat. 2943, 6 U.S. Code § 1504(b)(3)(D) (providing that guidelines under the statute for retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government shall, among other things, be consistent with the fair information practice principles set forth in appendix A of the document entitled "National Strategy for Trusted Identities in Cyberspace" and published by the President in April 2011), https://www.law.cornell.edu/uscode/text/6/1504. See also 6 U.S.C. § 142(a)(2), http://www.law.cornell.edu/uscode/text/6/142.

[38] See Paul M. Schwartz and Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 California Law Review 877, 877 (2014) ("The U.S. approach involves multiple and inconsistent definitions of PII that are often particularly narrow.").

[39] Federal Trade Commission, *Privacy Online: A Report to Congress* 7 (1998), http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf.

> (4) Security - Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.[40]

The 2000 FTC's version of FIPs includes only notice, choice, access and correction, and security. The FTC's 2000 set of privacy standards restates, waters down, and leaves out some FIPs elements. Curiously, the 2000 report references the 1998 report and, in one place but not another, mentions that the previous report identified *enforcement* as a "critical component". However, the 2000 report fails to include enforcement as a specific FIPs element, reducing the number of FIPs from five in the 1998 report to four in the 2000 report.[41] Then later, the report states that "[i]n addition to the substantive fair information practice principles of Notice, Choice, Access, and Security, a fifth principle is essential to ensuring consumer protection: Enforcement."[42] The inconsistent accounting of FIPs by the Commission in these two reports is curious.

A December 2010 FTC staff report appeared to acknowledge that the Commission's previous version of FIPs was incomplete and insufficient. It observed, "Additionally, the emphasis on notice and choice alone has not sufficiently accounted for other widely recognized fair information practices, such as access, collection limitation, purpose specification, and assuring data quality and integrity."[43] This comment adds *data quality and integrity* to what the Commission staff called a list of *widely recognized fair information practices*, but this list did not include enforcement. From 1998 through 2010, the Commission's description of FIPs has been consistently inconsistent.

### B. 2008 DHS

In 2008, the Privacy Office at the Department of Homeland Security offered its own version of FIPs called Fair Information Practice Principles (FIPPS):

> • Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
>
> • Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide

---

[40] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* 36-37, (May 2000) (footnote omitted), http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.
[41] Id. at 4.
[42] Id. at 20.
[43] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* 20 (2010) (Preliminary FTC Staff Report) 20, http://ftc.gov/os/2010/12/101201privacyreport.pdf. The comment appears to have vanished when the final report was published. See Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and PolicyMakers* (2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

• Purpose Specification: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

• Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

• Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

• Data Quality and Integrity: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

• Security: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

• Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.[44]

The DHS issuance is noteworthy for American statutory analysis since it implements the first statutory reference to fair information practices. The DHS FIPPs includes eight principles that match up closely but not precisely with the OECD version. Differences include: a) the replacement of the OECD Collection Limitation Principle with a Data Minimization Principle; b) the movement of some elements from one principle to another (e.g., the provision for obtaining data with the knowledge or consent of the data subject is part of the DHS Individual Participation Principle); c) elimination of the requirement for collection by fair and lawful means (DHS may have assumed that it only acts in lawful ways); d) some additional specificity appropriate for specific implementation with a particular organization (e.g., requiring employee and contractor training); and e) the addition of a requirement that DHS specifically articulate the authority that permits the collection of PII to the Purpose Specification principle. The last of these differences may be a reflection of the Privacy Act of 1974 requirement that each federal agency inform an individual of the authority that authorizes solicitation of information.[45]

---

[44] 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.
[45] 5 U.S.C. § 552a(e)(3)(A), http://www.law.cornell.edu/uscode/text/5/552a.

FIPs vs. FIPPS

It appears that the U.S. Department of Homeland Security first introduced *FIPPs* as a formal alternative label to *FIPs* for describing Fair Information Practices.[46] Earlier reports by the Federal Trade Commission in 1998 and 2000 (cited earlier) used Fair Information Practices with and without "Principles".

Some other U.S. agencies and a few organizations outside the federal government use FIPPs. The difference in labeling appears wholly one of style. While there are sometimes substantive differences between statements of *FIPPs* and classic statements of *FIPs*, the differences are no greater in degree or kind than differences among various statements of *FIPs*. Some traditionalists (including the author of this history), much prefer *FIPs* over *FIPPS*.

## C. 2011 NSTIC

In April 2011, the Obama White House included a version of FIPs in a report by the National Strategy for Trusted Identities in Cyberspace (NSTIC). This version is noteworthy because it came with the White House imprimatur and appears to be the first version of FIPs so endorsed. It is also clear that principles set out in the NSTIC report seek to guide private sector entities as well as government agencies that participate in the Report's recommended *Identity Ecosystem* for online identification and authentication. Thus, the NSTIC report is notable for the White House's extension of FIPPs to the private sector, at least in this context.

> • **Transparency**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
>
> • **Individual Participation**: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
>
> • **Purpose Specification**: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
>
> • **Data Minimization**: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

[46] 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.

> • **Use Limitation**: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
>
> • **Data Quality and Integrity**: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
>
> • **Security**: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
>
> • **Accountability and Auditing**: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.[47]

Like DHS, NSTIC calls its version FIPPs, and it is clear that NSTIC derived it from the DHS version. The differences with the DHS version are not explained, although most simply reflect the more general restatement of the principles for *organizations* rather than just for DHS. However, because of a revision of the Transparency Principle, there is no prior reference for *the notice* mentioned in the Use Limitation Principle. Also, the extension of the Purpose Specification Principle's requirement for stating the authority that permits the collection of PII may not be meaningful for all non-governmental activities.

### D. 2011 National Science and Technology Council

In June 2011, the White House released a second document that relied on FIPPs as a core policy. The National Science and Technology Council issued a report titled A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future.[48] The report outlines policy recommendations that build upon the Energy Independence and Security Act of 2007 and the Obama Administration's smart grid investments to foster long-term investment, job growth, innovation, and help consumers save money.

The report's policy framework rests on four pillars for a smarter grid: (a) enabling cost-effective smart grid investments; (b) unlocking the potential of innovation in the electric sector; (c) empowering consumers and enabling informed decision making; and (d) securing the grid from cybersecurity threats. One of the key actions for the third pillar provides:

> 10. State and Federal regulators should consider, as a starting point, methods to ensure that consumers' detailed energy usage data are protected in a manner consistent with Fair Information Practice Principles (FIPPs) and develop, as appropriate, approaches to address particular issues unique to energy usage. FIPPs

[47] National Strategy for Trusted Identities in Cyberspace, *Enhancing Online Choice, Efficiency, Security, and Privacy* at Appendix A (2011), https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf.
[48] https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

> are widely accepted principles adopted by government agencies and intergovernmental organizations to ensure protection of personal information. The Administration supports legislation that would make FIPPs the baseline for protecting personal data in commercial sectors not currently subject to sector specific Federal privacy statutes.

The report does not include a full statement of FIPPs, but it cites various other documents on FIPPs and it observes: *At present, there is not in place a comprehensive and broadly-accepted application of Fair Information Practice Principles (FIPPs) in the smart grid context*.[49]

## E. 2012 Department of Commerce

In February 2012, the White House issued yet another version of FIPPs in the context of a report on consumer privacy titled A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.[50] The Department of Commerce prepared the report.

The 2012 report included a Consumer Bill of Rights that "applies comprehensive, globally recognized Fair Information Practice Principles (FIPPs)."

The text of the Consumer Bill of Rights follows.

> The Consumer Privacy Bill of Rights applies to personal data, which means any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device. The Administration supports Federal legislation that adopts the principles of the Consumer Privacy Bill of Rights. Even without legislation, the Administration will convene multistakeholder processes that use these rights as a template for codes of conduct that are enforceable by the Federal Trade Commission. These elements—the Consumer Privacy Bill of Rights, codes of conduct, and strong enforcement—will increase interoperability between the U.S. consumer data privacy framework and those of our international partners.
>
> 1. **INDIVIDUAL CONTROL: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.** Companies should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data. Companies should enable these choices by providing consumers with easily used and accessible mechanisms that reflect the scale, scope, and sensitivity of the personal data that they collect, use, or disclose, as well as the sensitivity of the uses they make of personal data. Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure. Companies should offer consumers means to withdraw or limit

[49] Id. at 46.
[50] https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

consent that are as accessible and easily used as the methods for granting consent in the first place.

2. **TRANSPARENCY: Consumers have a right to easily understandable and accessible information about privacy and security practices.** At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.

3. **RESPECT FOR CONTEXT: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.** Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide heightened Transparency and Individual Choice by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults.

4. **SECURITY: Consumers have a right to secure and responsible handling of personal data.** Companies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure.

5. **ACCESS AND ACCURACY: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.** Companies should use reasonable measures to ensure they maintain accurate personal data. Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. Companies that handle personal data should

construe this principle in a manner consistent with freedom of expression and freedom of the press. In determining what measures, they may use to maintain accuracy and to provide access, correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm.

6. **FOCUSED COLLECTION: Consumers have a right to reasonable limits on the personal data that companies collect and retain.** Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise.

7. **ACCOUNTABILITY: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.** Companies should be accountable to enforcement authorities and consumers for adhering to these principles. Companies also should hold employees responsible for adhering to these principles. To achieve this end, companies should train their employees as appropriate to handle personal data consistently with these principles and regularly evaluate their performance in this regard. Where appropriate, companies should conduct full audits. Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise.

The White House/Department of Commerce report includes Appendix B (not reproduced here) that provides a chart that compares the proposed Consumer Bill of Rights with other statements of FIPPs. The other statements in the chart are the OECD Privacy Guidelines, the DHS privacy policy, and the APEC principles.

Much could be said about the proposed Consumer Bill of Rights. Analysis here is limited to a few points. First, this is the third document from the Obama White House that discusses and supports FIPs. The others are found (and discussed above) in the National Strategy for Trusted Identities in Cyberspace (NSTIC) and A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future. The Consumer Bill of Rights version differs from the version in the NSTIC report. The third version is too summary to characterize.

Second, the first principle on individual control appears to limit consumer rights to "personal data companies collect *from* consumers." It apparently does not cover information from other sources. This has the potential to greatly limit the rights of consumers with respect to personal data held by companies as much data comes from third parties.

Third, the context principle seems to significantly lessen the restrictions found in the OECD principle of Use Limitation, which requires data subject consent or legal authority to change the

uses specified. The Consumer Bill of Rights casts the policy in terms of "purposes that are consistent with the relationship between the consumer and a company" and "the context in which consumers originally disclosed the data." The means of each of these phrases is far from clear. The context principle is not the only one in the Consumer Bill of Rights where the associated commentary apparently undermines the top-level principles.

Fourth, the White House sought legislation adopting the Consumer Privacy Bill of Rights. However, translating the top-level principles into legislation is not a simple task. Some questioned the bona fides of the Commerce Department in consumer privacy matters. See, e.g., World Privacy Forum, The US Department of Commerce and International Privacy Activities: Indifference and Neglect (2010).[51]

## F. 2012 FTC

The Federal Trade Commission issued a major report about privacy in 2012. The report appears to support a framework that the Commission asserts is "consistent with the Fair Information Practice Principles first articulated almost 40 years ago."[52] However, the text quoted in the last sentence immediately offers these principles:

> • **Privacy by Design:** Build in privacy at every stage of product development
>
> • **Simplified Choice for Businesses and Consumers:** Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism, while reducing the burden on businesses of providing unnecessary choices; and
>
> • **Greater Transparency:** Make information collection and use practices transparent.[53]

The Commission's privacy framework is set out here, without the legislation recommendations or the Commission's implementation plans.

> SCOPE
>
> **Final Scope:** The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only nonsensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.
>
> PRIVACY BY DESIGN

---

[51] http://www.worldprivacyforum.org/permalink/permalinknov222010.html.
[52] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* Executive Summary at i (2012), http://ftc.gov/os/2012/03/120326privacyreport.pdf.
[53] Executive Summary at i.

**Baseline Principle:** Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

A. The Substantive Principles

**Final Principle:** Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

B. Procedural Protections to Implement the Substantive Principles

**Final Principle:** Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

SIMPLIFIED CONSUMER CHOICE

**Baseline Principle:** Companies should simplify consumer choice.

A. Practices That Do Not Require Choice

**Final Principle:** Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law. To balance the desire for flexibility with the need to limit the types of practices for which choice is not required, the Commission has refined the final framework so that companies engaged in practices consistent

B. Companies Should Provide Consumer Choice for Other Practices

**Final Principle:** For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes. The Commission commends industry's efforts to improve consumer control over online behavioral tracking by developing a Do Not Track mechanism, and encourages continued improvements and full implementation of those mechanisms.

TRANSPARENCY

**Baseline Principle:** Companies should increase the transparency of their data practices.

A. Privacy notices

> **Final Principle:** Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.
>
> B. Access
>
> **Final Principle:** Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use. The Commission has amplified its support for this principle by including specific recommendations governing the practices of information brokers.
>
> C. Consumer Education
>
> **Final Principle:** All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.[54]

While transparency is a classic FIPs principle, neither Privacy by Design nor Simplified Choice reflects the full FIPs principles. The word *choice* does not appear in the classic OECD formulation of FIPs. It is unclear from the report whether the Commission is embracing FIPs or restating FIPs. It is unclear whether other FIPs principles not mentioned were abandoned or just ignored. The Commission is under no obligation to take a position on FIPs or to state whether its framework satisfies FIPs standards. Its characterization of *consistency* with FIPs is ambiguous, probably quite deliberately so.

The Commission is another in an increasingly long list of producers of privacy principles that sought in some way to suggest that its principles align in some way with the classic statement of FIPs without necessarily supporting all of the classic principles. FIPs may have become a form of generic trademark for privacy principles rather than an indicator of any affiliation with the original standards.

## G. 2012 HHS ONC Principles

The Department of Health and Human Services has a variety of health technology and health privacy responsibilities. Some form of FIPs appears to the basis for policy, but it is not clear that the Department relies on a clear and consistent version of FIPs.

The Office of the National Coordinator for Health Information Technology (ONC) located in the Department of Health and Human Services used a version of Fair Information Practice Principles. The ONC version of FIPs was included in a 2008 document on the electronic exchange of individually identifiable health information:

> **II. The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information**

[54] Id. at vii-viii.

*SCOPE*

*These principles are expected to guide the actions of all health care-related persons and entities that participate in a network for the purpose of electronic exchange of individually identifiable health information. These principles are not intended to apply to individuals with respect to their own individually identifiable health information.*

*INTRODUCTION*

Adoption of privacy and security protections is essential to establishing the public trust necessary for effective electronic exchange of individually identifiable health information. A common set of principles that stakeholders accept and support is the first step towards realizing those privacy and security protections and establishing the necessary public trust. The approach of developing principles to guide information practices while advancing technology was marked by the 1973 release of the Code of Fair Information Practice and has been the basis for various activities in the public and private sectors, including the development of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and as the basis for this framework.

The implementation of these principles should evolve in concert with technological advances that allow for greater protections. Adherence should be the responsibility of each health care-related person or entity that holds and exchanges electronic individually identifiable health information through a network, as well as the responsibility of other persons and entities that receive or have access to such information, so that electronic individually identifiable health information is protected at all times.

These principles do not constitute legal advice and do not affect a person's or entity's duty to comply with applicable legal requirements. Where these principles set higher standards than legal requirements, adherence to these principles is encouraged.

**INDIVIDUAL ACCESS**

Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.

*Access to information enables individuals to manage their health care and well-being. Individuals should have a reasonable means of access to their individually identifiable health information. Individuals should be able to obtain this information easily, consistent with security needs for authentication of the individual; and such information should be provided promptly so as to be useful*

*for managing their health. Additionally, the persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide such information in a readable form and format, including an electronic format, when appropriate. In limited instances, medical or other circumstances may result in the appropriate denial of individual access to their health information.*

**CORRECTION**

Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

*Individuals have an important stake in the accuracy and integrity of their individually identifiable health information and an important role to play in ensuring its accuracy and integrity. Electronic exchange of individually identifiable health information may improve care and reduce adverse events. However, any errors or conclusions drawn from erroneous data may be easily communicated or replicated (e.g., as a result of an administrative error as simple as a transposed digit or more complex error arising from medical identity theft). For this reason it is essential for individuals to have practical, efficient, and timely means for disputing the accuracy or integrity of their individually identifiable health information, to have this information corrected, or a dispute documented when their requests are denied, and to have the correction or dispute communicated to others with whom the underlying information has been shared. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should make processes available to empower individuals to exercise a role in managing their individually identifiable health information and should correct information or document disputes in a timely fashion.*

**OPENNESS AND TRANSPARENCY**

There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

*Trust in electronic exchange of individually identifiable health information can best be established in an open and transparent environment. Individuals should be able to understand what individually identifiable health information exists about them, how that individually identifiable health information is collected, used, and disclosed and whether and how they can exercise choice over such collections, uses, and disclosures. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review*

*who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format. Notice of policies, procedures, and technology-- including what information will be provided under what circumstances -- should be timely and, wherever possible, made in advanced of the collection, use, and/or disclosure of individually identifiable health information. Policies and procedures developed consistent with this Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information should be communicated in a manner that is appropriate and understandable to individuals.*

**INDIVIDUAL CHOICE**

Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.

*The ability of individuals to make choices with respect to electronic exchange of individually identifiable health information concerning them is important to building trust. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities and capabilities for individuals to exercise choice with respect to their individually identifiable health information. The degree of choice made available may vary with the type of information being exchanged, the purpose of the exchange, and the recipient of the information. Applicable law, population health needs, medical necessity, ethical principles, and technology, among other factors, may affect options for expressing choice. Individuals should be able to designate someone else, such as a family member, care-giver, or legal guardian, to make decisions on their behalf. When an individual exercises choice, including the ability to designate someone else to make decisions on his or her behalf, the process should be fair and not unduly burdensome.*

**COLLECTION, USE, AND DISCLOSURE LIMITATION**

Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.

*Establishing appropriate limits on the type and amount of information collected, used, and/or disclosed increases privacy protections and is essential to building trust in electronic exchange of individually identifiable health information because it minimizes potential misuse and abuse. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should only collect, use, and/or disclose information necessary to accomplish a specified purpose(s). Persons and entities*

*should take advantage of technological advances to limit data collection, use, and/or disclosure.*

**DATA QUALITY AND INTEGRITY**

Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.

*The completeness and accuracy of an individual's health information may affect, among other things, the quality of care that the individual receives, medical decisions, and health outcomes. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, have a responsibility to maintain individually identifiable health information that is useful for its intended purposes, which involves taking reasonable steps to ensure that information is accurate, complete, and up-to-date, and has not been altered or destroyed in an unauthorized manner. Persons and entities have a responsibility to update or correct individually identifiable health information and to provide timely notice of these changes to others with whom the underlying information has been shared. Moreover, persons and entities should develop processes to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information.*

**SAFEGUARDS**

Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

*Trust in electronic exchange of individually identifiable health information can only be achieved if reasonable administrative, technical, and physical safeguards are in place to protect individually identifiable health information and minimize the risks of unauthorized or inappropriate access, use, or disclosure. These safeguards should be developed after a thorough assessment to determine any risks or vulnerabilities to individually identifiable health information. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should implement administrative, technical, and physical safeguards to protect information, including assuring that only authorized persons and entities and employees of such persons or entities have access to individually identifiable health information. Administrative, technical, and physical safeguards should be reasonable in scope and balanced with the need for access to individually identifiable health information.*

**ACCOUNTABILITY**

> These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate nonadherence and breaches.
>
> *These nationwide privacy and security principles will not be effective in building trust in electronic exchange of individually identifiable health information unless there is compliance with these Principles and enforcement mechanisms. Mechanisms for assuring accountability include policies and procedures and other tools. At a minimum, such mechanisms adopted by persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should address: (1) monitoring for internal compliance including authentication and authorizations for access to or disclosure of individually identifiable health information; (2) the ability to receive and act on complaints, including taking corrective measures; and (3) the provision of reasonable mitigation measures, including notice to individuals of privacy violations or security breaches that pose substantial risk of harm to such individuals*.[55]

While not labelled expressly in the document as FIPs, the principles look mostly like FIPs. There are eight principles, although collection limitation is oddly grouped with use and disclosure limitation, and access and correction (often called *individual participation*) have been separated into two separate principles. Choice is not a classic FIPs principle.

The Office for Civil Rights at HHS is responsible for implementation and enforcement of the health privacy and security rules under HIPAA. At an OCR website on *Health Information Technology*, OCR sets out a *Privacy and Security Framework*.[56] The Framework has six elements:

> CORRECTION PRINCIPLE: Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.
>
> OPENNESS AND TRANSPARENCY PRINCIPLE: There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.
>
> INDIVIDUAL CHOICE PRINCIPLE: Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.

---

[55] Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, *Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information* (Dec. 15, 2008), https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.
[56] https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html.

> COLLECTION, USE, AND DISCLOSURE LIMITATION PRINCIPLE: Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
>
> SAFEGUARDS PRINCIPLE: Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
>
> ACCOUNTABILITY PRINCIPLE: The Principles in the Privacy and Security Framework should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

These elements sometimes use the same language as the 2008 ONC principles, sometimes offer similar policies in different words, and sometimes leave out statements found in the ONC principles. Oddly, the OCR framework does not expressly address the data integrity or access principles identified by ONC.

In March 2012, the Centers for Medicare and Medicaid (CMS), which is part of HHS, published a final rule regarding affordable insurance exchanges consistent with the Patient Protection and Affordable Care Act of 2010, as amended by the Health Care and Education Reconciliation Act of 2010.[57] The rule is long and complex, but for present purposes, it "includes privacy and security principles based on the Fair Information Practice Principles (FIPPs) framework adopted by ONCHIT."[58] The adopted principles are:

> (i) Individual access. Individuals should be provided with a simple and timely means to access and obtain their personally identifiable health information in a readable form and format.
>
> (ii) Correction. Individuals should be provided with a timely means to dispute the accuracy or integrity of their personally identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied.
>
> (iii) Openness and transparency. There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable health information.
>
> (iv) Individual choice. Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their personally identifiable health information.

---

[57] 77 Federal Register 18310 (March 27, 2012), http://www.gpo.gov/fdsys/pkg/FR-2012-03-27/pdf/2012-6125.pdf.
[58] Id. at 18436.

> (v) Collection, use, and disclosure limitations. Personally identifiable health information should be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
>
> (vi) Data quality and integrity. Persons and entities should take reasonable steps to ensure that personally identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
>
> (vii) Safeguards. Personally identifiable health information should be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
>
> (viii) Accountability. These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

In comparing the CMS principles with the ONC principles and the OCR principles, the CMS principles are the same in some respects, broader in part, shorter in part, and different in part. At a high enough level of abstraction, there is much similarity in these three sets of principles. Yet there are clear and substantive policy differences at a secondary level. A detailed comparison of the three versions is left to the reader. The hardest part to understand is the absence of two entire principles from the OCR website. If there is a purpose behind the same Department offering three different versions of FIPs, it is not clear.

Overall, the number of versions of FIPs appears to increase with every repetition. Because FIPs are high-level principles, implementation in different contexts may differ. Often, the commentary accompanying the principles includes more details and more shaping to fit the context. The commentary may make some of the difference noted here to be more or less significant. However, the variation at the higher level of principle remains curious.

If the differences are purposeful, that purpose is not explained anywhere. During the Obama Administration alone, we find different versions of FIPs produced by NSTIC, by the Department of Commerce, and at least two versions from HHS (with another version left over from the previous Administration). The DHS FIPPS slightly predates the Obama Administration, but it remains in place and differs from all the rest. The FTC is an independent agency, and its version of FIPs (if it actually qualified as a version of FIPs) cannot be attributed to the Obama Administration. The National Science and Technology Council may have come the closest to the truth when it said, "At present, there is not in place a comprehensive and broadly-accepted application of Fair Information Practice Principles (FIPPs) in the smart grid context." That statement appears to be true in other U.S. contexts. The lack of agreement within the same Administration and even within the same agency is noteworthy. The most likely explanation is that FIPs principles expand or contract with each writer and each application. The lack of any central privacy policy apparatus may be a contributing cause.

## H. 2013 Executive Order on Improving Critical Infrastructure Cybersecurity

On February 12, 2013, President Obama issued Executive Order 13636 on critical infrastructure cybersecurity.[59] The order broadly directs federal agencies to share more cyber threat information with the private sector. This is apparently the first Executive Order to reference FIPs, and it uses a version of FIPs previously referenced in a White House NTSIC document.

The order tells agencies to "coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities."[60] The required protections "shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities."[61] For purposes of the Executive Order, *Fair Information Practice Principles* means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.[62]

## I. OMB Guidance for Providing and Using Administrative Data for Statistical Purposes

In February 2014, the Office of Management and Budget issued guidance to promote more interagency data sharing for statistical purposes.[63] OMB argues that increased use of administrative data for statistical purposes can generate a range of benefits. The guidance includes an appropriate discussion of legal responsibilities for protecting privacy. The discussion of policies for privacy and confidentiality cites the Administration's proposal for Fair Information Practice Principles (FIPPs) as a framework for those policies. The guidance cites to the White House National Strategy for Trusted Identities in Cyberspace (April 2011).[64]

## J. Obama White House Big Data Report

In May 2014, the Executive Office of the President issued a report titled *Big Data: Seizing Opportunities, Preserving Values*.[65] The report included a brief history of FIPs, noting that "FIPPs form a common thread through these sectoral laws and a variety of international agreements."[66] The report referenced the Department of Commerce's 2012 privacy report's reliance on FIPPs.[67] Interestingly, a companion report issued at the same time by the President's

---

[59] http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[60] Id. at § 4(a).
[61] Id. at § 5.
[62] Id. at § 11(c).
[63] Memorandum M-14-06, https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-06.pdf.
[64] An earlier OMB memorandum, *Sharing Data While Protecting Privacy*, directed agencies to consult with established codes of FIPs, and the memo directed agencies to the original HEW report. Id. at text accompanying note 3.
[65] https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[66] Id. at 18.
[67] Id. at 61.

Council of Advisors on Science and Technology referenced a Federal Trade Commission version of FIPs from 2000 that included only four principles.[68]

## K. OMB Circular A-130

In July 2016, the Obama Administration revised Office of Management and Budget Circular A-130 on Managing Information as a Strategic Resource.[69] For the first time, the 2016 version of the circular mentions fair information practices principles. Appendix II of the Circular on Responsibilities for Managing Personally Identifiable Information includes section 3 setting out Fair Information Practice Principles. The Circular states:

> The Fair Information Practice Principles (FIPPs) are a collection of widely accepted principles that agencies should use when evaluating information systems, processes, programs, and activities that affect individual privacy. The FIPPs are not OMB requirements; rather, they are principles that should be applied by each agency according to the agency's particular mission and privacy program requirements.

This directive tells each agency to apply the principles according to the agency's mission and privacy program requirements. The Circular provides this statement of FIPPs, which appears here with the original footnotes:

> a. Access and Amendment. Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII. Fn 116.
>
> b. Accountability. Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.
>
> c. Authority. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice. Fn 117.
>
> d. Minimization. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose. Fn 118.

---

[68] President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective* (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[69] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

e. Quality and Integrity. Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

f. Individual Participation. Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

g. Purpose Specification and Use Limitation. Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

h. Security. Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

i. Transparency. Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII. Fn 119.

116 The Access and Amendment principle is included as part of the "Individual Participation" privacy control family in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems*. OMB is including Access and Amendment as a stand-alone principle in this Circular to emphasize the importance of allowing individuals to access and amend their information when appropriate.
117 The Authority principle is included as part of the "Purpose Specification" privacy control family in NIST SP 8053, Security and Privacy Controls for Federal Information Systems. OMB is including Authority as a stand-alone principle in this Circular to emphasize the importance of identifying a specific authority for creating, collecting, using, processing, storing, maintaining, disseminating, or disclosing PII.
118 In some versions of the FIPPs, the "minimization" principle is referred to under a different name, such as "collection limitation."
119 In some versions of the FIPPs, the "transparency" principle is referred to under a different name, such as "openness." [70]

The 2016 OMB version of FIPPs differs in modest ways from all other versions of FIPs, including those used by federal agencies in recent years. It also differs from other versions of FIPs used or referenced by other Obama White House documents. The Circular's footnotes seem to highlight or explain some of the differences.

[70] Id. at Appendix II.

In Circular A-130, OMB continues what might be called the common Obama Administration practice of restating FIPs with each new document. OMB attempted to explain some of the differences and some of its reasoning. In the end, the differences appear minor, and it is unknown if agencies will change their own versions of FIPPs to conform to the new OMB policy. The revision of Circular A-130 came in the last year of the Obama Administration. OMB circulars of this type are not commonly revised by an incoming Administration, but the option for change always remains. The last revision of A-130 occurred in 2000.

It is important to remember that the policy in Circular A-130 applies primarily to federal agencies. The Circular does not set general policies applicable to private sector activities except insofar as the private sector undertakes work for federal agencies to carry out government functions.

## L. NIST Privacy Engineering and Risk Management in Federal Systems

A January 2017 document from the National Institute of Standards and Technology at the U.S. Department of Commerce offers an introduction to the concepts of privacy engineering and risk management for federal systems. It offers approaches and guidelines for "translating widely recognized, high-level privacy principles – such as the Fair Information Practice Principles (FIPPs) – into effective system privacy requirements."[71]

## M. Energy Act of 2020

The Energy Act of 2020, enacted as part of the Consolidated Appropriations Act, 2021, included a reference to FTC FIPs:

> (7) PROTECTING PRIVACY AND SECURITY.—In carrying out this subsection, the Secretary shall identify, incorporate, and follow best practices for protecting the privacy of individuals and businesses and the respective sensitive data of the individuals and businesses, including by managing privacy risk and implementing the Fair Information Practice Principles of the Federal Trade Commission for the collection, use, disclosure, and retention of individual electric consumer information in accordance with the Office of Management and Budget Circular A-130 (or successor circulars).[72]

As documented in this history, the FTC adopted various versions of FIPs at different times. OBM Circular A-130, also referenced in the statute, offers a version of FIPs that differs from the FTC's versions. Resolving the statutory references and reconciling the multiple standards of FIPs may not be simple, but it may not be overly important either if the requirement is taken as a general direction to pay attention to privacy.

---

[71] National Institute of Standards and Technology, An Introduction to Privacy Engineering and Risk Management in Federal Systems (2017) (NISTIR 8062), https://doi.org/10.6028/NIST.IR.8062. A later document on the subject, Risk Management Framework for Information Systems and Organizations, NIST Special Publication 800-37 Revision 2 (2018) does not appear to mention Fair Information Practices, https://doi.org/10.6028/NIST.SP.800-37r2.
[72] Public Law 116-260, § 3201(b)(7), https://www.congress.gov/bill/116th-congress/house-bill/133/text/pl.

## V. Comment and Criticism about FIPs

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; privacy impact assessments; and other methods. Similarly, providing data subjects with access to their own records may have different exceptions, depending on whether the records are employment, educational, credit, or law enforcement records. Implementation of FIPs in any context is often more a matter of art and judgment rather than a science or mechanical translation of principles.

In a 2001 article, Marc Rotenberg wrote about the spread of FIPs and the international convergence around FIPs.

> Not only have Fair Information Practices played a significant role in framing privacy laws in the United States, these basic principles have also contributed to the development of privacy laws around the world and even to the development of important international guidelines for privacy protection. The most well-known of these international guidelines are the Organization for Economic Co-operation and Development's Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines"). The OECD Guidelines set out eight principles for data protection that are still the benchmark for assessing privacy policy and legislation: Collection Limitation; Data Quality; Purpose Specification; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability. The principles articulate in only a couple of pages a set of rules that have guided the development of national law and increasingly the design of information systems.
>
> It is generally understood that the challenge of privacy protection in the information age is the application and enforcement of Fair Information Practices and the OECD Guidelines. While some recommendations for improvement have been made, the level of consensus, at least outside of the United States, about the viability of Fair Information Practices as a general solution to the problem of privacy protection is remarkable. As recently as 1998 the OECD reaffirmed support for the 1980 guidelines, and countries that are adopting privacy legislation have generally done so in the tradition of Fair Information Practices.
>
> While some commentators have made recommendations for updating or expanding the principles, there is general agreement that the concept of Fair Information Practices and the specific standards set out in the OECD Guidelines continue to provide a useful and effective framework for privacy protection in information systems.

> Commentators have also noted a remarkable convergence of privacy policies. Countries around the world, with very distinct cultural backgrounds and systems of governance, nonetheless have adopted roughly similar approaches to privacy protection. Perhaps this is not so surprising. The original OECD Guidelines were drafted by representatives from North America, Europe, and Asia. The OECD Guidelines reflect a broad consensus about how to safeguard the control and use of personal information in a world where data can flow freely across national borders. Just as it does today on the Internet.[73]

Paula Bruening, a longstanding member of the international privacy community and formerly Senior Counsel, Global Privacy Policy, at Intel, offered an important observation about FIPs in a 2014 blog post. She observed that FIPs provide a *common language* of privacy that provides value to all, regardless of their particular implementation of privacy principles.

> Over time it's become clear that attempts to impose the privacy sensibilities or protection regimes of one country or region onto another usually meet with frustration. But internationally recognized, fundamental principles of fair information practices continue to provide a common language about data protection and privacy that has served nations, regions, companies and individuals around the world, without demanding a departure from local privacy values. And when there is a privacy or data protection failure, they provide a tool to measure compliance and a means of enforcement.[74]

Australian Law Professor Graham Greenleaf,[75] a privacy scholar and prolific author, collects and publishes information about privacy laws around the world.[76] In a 2012 article, Greenleaf offers a useful perspective on the influence of basic privacy policy principles like FIPs on privacy laws around the world.[77] He finds ten elements common to all four international privacy instruments (the OECD Guidelines, Council of Europe Convention, EU Data Protection Directive, and the APEC Privacy Framework:

1. Collection - limited, lawful and by fair means; with consent or knowledge
2. Data quality – relevant, accurate, up-to-date
3. Purpose specification at time of collection
4. Notice of purpose and rights at time of collection

---

[73] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)*, 2001 Stan. Tech. L. Rev. 1 (2001) (footnotes omitted), https://heinonline.org/HOL/LandingPage?handle=hein.journals/stantlr2001&div=2&t=1561532582.

[74] Paula Bruening, Rethink Privacy 2.0 and Fair Information Practice Principles: A Common Language for Privacy (2014), Blogs@Intel, http://blogs.intel.com/blog/rethink-privacy-2-0-and-fair-information-practice-principles-a-common-language-for-privacy/. Bruening also observed: "The challenge lies in understanding how fair information practice principles can be applied in an effective, workable way in the cloud, across the Internet of Things, and for big data analytics. It's a challenge we must meet." Id.

[75] http://www2.austlii.edu.au/~graham/.

[76] See *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*, UNSW Law Research Paper No. 2013-40, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877.

[77] Graham Greenleaf, *The influence of European data privacy standards outside Europe: Implications for Globalisation of Convention 108* (2011), 2 International Data Privacy Law (2012), http://ssrn.com/abstract=1960299.

5. Uses limited (including disclosures) to purposes specified or compatible
6. Security through reasonable safeguards
7. Openness re personal data practices
8. Access – individual right of access
9. Correction – individual right of correction
10. Accountable – data controllers accountable for implementation[78]

These are the basic FIPs principles restated into ten rather than eight elements. Greenleaf observes that "[t]here are often exception to, and variations of, these elements, but in one form or another, they are always found."[79] This underscores Bruening's observation about FIPs as the common language of privacy.

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 weaknesses of self-regulation, and have not kept pace with information technology.[80] 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. Some argue that the supposed benefits of so-called Big Data mean that the collection limitation principle should be weakened or abandoned. Daniel Solove and Chris Hoofnagle offer a different tack, a model regime of privacy protection based on FIPs with more specificity.[81]

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.

---

[78] Id. at 7.
[79] Id.
[80] 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.
[81] Daniel J. Solove and Chris Jay Hoofnagle, *A Model Regime of Privacy Protection (Version 3.0)*, 2006 University of Illinois Law Review 357 (2006), http://ssrn.com/abstract=881294.

> 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.[82]

The 2013 revisions of the OECD Privacy Guidelines did not appear to address any of the new rights suggested by Mr. Justice Kirby.

As a result of the 2014 decision of the European Court of Justice in the *Google* Spain case, some suggest that the so-called right to be forgotten might be another new right.[83] The right to be forgotten may be similar to Mr. Justice Kirby's suggested right not to be indexed.

The Open Identity Exchange published (under a Creative Commons license) a *Fair Information Practice Principles (FIPPs) Comparison Tool*. This document list FIPs principles by subject rather than by source, and it includes principles from more than a dozen sources. This presentation will be useful to many with an interest in FIPs. Appendix 2 to the document is noteworthy for its "extended discussion of how the FIPPs tool can help parties engaged in current trust framework development and drafting and in future legal standardization efforts, and its relationship to other trust framework development tools and processes." http://openidentityexchange.org/wiki/fair-information-practice-principles-fipps-comparison-tool.

On the thirtieth anniversary of the OECD Guidelines, the OECD held a conference on the impact of the Guidelines, sponsored several roundtables, and commissioned papers.[84] Mr. Justice Michael Kirby was one of the participants, and his speech gives new insight on the origins of the original Guidelines and on new challenges, which include new systems of mass surveillance; the need for privacy enhancing technologies; cross-border cooperation in drafting, implementation, and enforcement; end user education; and including developing nations in privacy discussions.[85]

Other information and documents pertaining to the 30th anniversary of the OECD Guidelines are available.[86] Of particular note is an April 2011 OECD paper titled *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*. The paper offers a review of the development and influence of the Guidelines, describes current trends in the processing of personal data and the privacy risks, and concludes that the "OECD Privacy Guidelines have been a remarkable success."[87] The 2011 paper was included with the 2013 revisions of the OECD Privacy Guidelines.

---

[82] Michael Kirby, *Privacy Protection – A New Beginning*, (1999) (speech before the 21st International Conference on Privacy and Personal Data Protection), http://www.austlii.edu.au/au/journals/PLPR/1999/41.html.
[83] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, ECLI:EU:C:2014:317 (Case C-131/12), http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d55d64d9a37b5a477eac11d72c1de1eb84.e34KaxiLc3qMb40Rch0SaxuNb3z0?text=&docid=152065&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=265967.
[84] https://www.oecd.org/digital/ieconomy/the30thanniversaryoftheoecdprivacyguidelines.htm.
[85] The speech can be found on this page: https://www.oecd.org/sti/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm.
[86] https://www.oecd.org/sti/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm.
[87] www.oecd-ilibrary.org/science-and-technology/the-evolving-privacy-landscape-30-years-after-the-oecd-privacy-guidelines_5kgf09z90c31-en or https://doi.org/10.1787/5kgf09z90c31-en.

At the 30th anniversary event, Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, identified nine factors that contributed to the initial success of the OECD Guidelines: 1) The OECD Guidelines were forward-looking; 2) The Guidelines were narrow in scope and focused on a particular problem; 3) The Guidelines were intellectually coherent; 4) The Guidelines were technologically neutral; 5) The Guidelines have an institutional home; 6) There was at the outset broad participation from countries around the world; 7) The Guidelines had a champion; 8) Expertise of Committee; and 9) The Guidelines had the right level of specificity.[88]

Rotenberg, along with law professor Anita Allen, offers comments on the history, background, and importance of FIPs in their casebook Privacy Law and Society.[89] The comments are worth reproducing here in their entirety. Note especially the last paragraph discussion that sees *notice and choice* as a mechanism for waiver of privacy and not a regime for privacy protection.

> (3) Fair Information Practices
>
> The concept of Fair Information Practices ("FIPs") has powerfully influenced the development of modern privacy law. Simply stated, Fair Information Practices set out the rights and responsibilities for the collection and use of personal data. First set out in a 1973 report, Records, Computers, and the Rights of Citizens, "Fair Information Practices" describe the basic architecture of modern privacy law. These requirements for collection and use of personal data provided the basis for the Privacy Act of 1974, the most comprehensive US privacy law, as well as many other modern privacy laws.
>
> There are many conceptions of FIPs, but they all share a common architecture, assigning rights and responsibilities to data subjects and data holders. That is the overarching concept. See generally Ronald Dworkin, **Taking Rights Seriously** 134–36 (1978) (describing the relationship between concepts and conceptions in legal reasoning.)
>
> Willis Ware, the chair of the 1973 government advisory group that produced the report "*Records, Computers, and the Rights of Citizens*" is generally credited with the creation of the original Fair Information Practices. He analogized to the Fair Labor Standards Act of 1938 which established minimum wage, overtime pay eligibility, recordkeeping, and child labor standards for all employment in the public and private sector. The FLSA was drafted in 1932 by Senator Hugo Black, who was later appointed to the Supreme Court in 1937. President Franklin Roosevelt called the Fair Labor Standards Act the most important piece of New Deal legislation since the Social Security Act of 1935. See Wikipedia, "Fair Labor Standards Act."

---

[88] www.oecd.org/internet/ieconomy/44946274.doc. [This link does not work consistently. You can also find it through https://www.oecd.org/sti/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm.]
[89] At 755-57. See http://privacylawandsociety.org/.

Note that the emphasis in both the FLSA and the FIPs is on actual practices or standards, as well as legal rights. In recent years, many have misunderstood the origins and purpose of the FIPs, referring to the concept as "Fair Information Practices Principles." But FIPPs convey an aspirational tone that is at odds with fundamental legal obligations. Just as companies that hire employees are subject to the FLSA, Ware believed that organizations that collect and use personal data would be subject to enforceable FIPs. Actual practices not principles is the core aim.

The original HEW Report of 1973 set out five requirements for the collection and use of personal data. The influential OECD Privacy Guidelines of 1980 contained eight requirements. How did this change come about? The answer is found in the 1977 report of the Privacy Protection Study Commission of which explained:

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)
(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)

Each of these principles is manifest in one or more of the Privacy Act's specific requirements, and in their application they all require a balancing of individual, organizational, and societal interests. Privacy Protection Study Commission, Personal Privacy in an Information Society, ch. 13 (1977).

Note that neither "Notice" or "Choice" appears in the original articulation of Fair Information Practices or in the restatement described by the PPSC or the OECD

> Privacy Guidelines. This recent reformulation, like "Fair Information Practices Principles," misunderstands the history and purpose of Fair Information Practices. The key to modern privacy law is that the obligations associated with the collection and use of personal data are ongoing. From this perspective, "notice and choice" operates as a waiver or disclaimer, a mechanism to obtain consent for the use of personal data, not a regime for privacy protection. See Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stanford Technology Law Review 1 (2001).

Continuing support for FIPs among public interest and civil society groups is evidenced by the November 2009 Madrid Privacy Declaration.[90] The declaration emerged from a meeting of the Public Voice Coalition held in conjunction with the annual meeting of the International Privacy and Data Protection and Commissioners. The Declaration, which has attracted signatures from over 300 groups, experts, and individuals, "[reaffirms] support for a global framework of Fair Information Practices that places obligations on those who collect and process personal information and gives rights to those whose personal information is collected." Other parts of the Declaration support independent data protection authorities, call for ratification of Council of Europe Convention 108, and seek better legal frameworks for privacy protection, among other things.

Greenleaf's analysis identified additional "European" elements that are indicative of higher (or stricter) standards that the EU Directive, the Council of Europe Convention, or both include:

> 1. Requirement of an independent Data Protection Authority as the key element of an enforcement regime
> 2. Requirement of recourse to the courts to enforce data privacy rights
> 3. Requirement of restrictions on personal data exports to countries which did not have a sufficient standard of privacy protection (defined as 'adequate')
> 4. Collection must be the minimum necessary for the purpose of collection, not simply 'limited'
> 5. A general requirement of 'fair and lawful processing' (not just collection)
> 6. Requirements to notify, and sometimes provide 'prior checking', of particular types of processing systems
> 7. Destruction or anonymisation of personal data after a period
> 8. Additional protections for particular categories of sensitive data
> 9. Limits on automated decision-making, and a right to know the logic of automated data processing
> 10. Requirement to provide 'opt-out' of direct marketing uses of personal data.[91]

---

[90] http://thepublicvoice.org/madrid-declaration.

[91] Graham Greenleaf, *The influence of European data privacy standards outside Europe: Implications for Globalisation of Convention 108* (2011), 2 International Data Privacy Law 8 (2012), http://ssrn.com/abstract=1960299. Greenleaf observes that this list is not exhaustive. Greenleaf's article appeared before the OECD issued its revised guidelines in 2013. As noted above, the revisions did not change the eight basic principles, but the OECD 2013 document introduced new concepts to the privacy framework, some of which overlap with Greenleaf's European elements.

None of these ten elements is required by the original OECD Guidelines, but many can be found in whole or in part in national privacy laws today. Greenleaf offers the list of European elements for several purposes, including a comparison with the APEC Privacy Framework, which lacks all of them.[92]

Greenleaf's list of higher privacy standards illustrates the recent evolution of privacy policy. This is not so much criticism that FIPs are outdated but that FIPs are no longer sufficient to address current needs. FIPs have not been abandoned or superseded in favor of the newer privacy elements. FIPs remain as foundational principles in privacy laws everywhere. It would be more accurate to say that technology, administrative developments, and a better understanding of what is needed to protect privacy are adding elements beyond FIPs to international privacy policy discussions, debates, standards, and laws.

A more recent Greenleaf paper raises the notion of other, additional privacy standards.

> The international standards for a data privacy law continue to evolve, and the new models for where such standards could be found have generally been regarded as the EU's General Data Protection Regulation (GDPR) and the [Council of Europe's] "modernised" Convention 108 (now known as 108+).[93]

Greenleaf suggests that there may be "third-generation" principles evolving as privacy laws evolve. He mentions features of California law that do not have equivalents in the GDPR, including stronger deletion rights, no retaliation for exercise of rights, right to opt-out of behavioral advertising.

Whether the features of newer laws rise to the level of new principles or are implementation of existing principles remains to be seen. For example, requirement for an independent data protection authority clearly is a core element of privacy law today, but it can also be seen as an implementation of the FIPs accountability principle. A distinction between principle and implementation may be mostly academic in the end.

Law professor Woody Herzog essentially makes the same points that Greenleaf makes about the importance of FIPs and the need to go further:

> For the past thirty years, the general advice for those seeking to collect, use, and share people's personal data in a responsible way was relatively straightforward: follow the fair information practices, often called the "FIPs." These general guidelines were designed to ensure that data processors are accountable for their actions and that data subjects are safe, secure, and endowed with control over their personal information. The FIPs have proven remarkably sturdy against the backdrop of near-constant technological change. Yet in the age of social media,

---

[92] See also Graham Greenleaf, ASIAN DATA PRIVACY LAWS Trade & Human Rights Perspectives (2014), https://global.oup.com/academic/product/asian-data-privacy-laws9780199679669?cc=us&lang=en&.

[93] Graham Greenleaf, *California's CCPA 2.0: Does the US finally have a data privacy Act?*, 168 Privacy Laws & Business International Report 13-17 (2020), https://www.privacylaws.com/reports (paywall). This paper may appear soon at SSRN.com.

> big data, and artificial intelligence, the FIPs have been pushed to their breaking point. We are asking too much of the FIPs, yet they are far too entrenched and important to be abandoned.[94]

Professor Herzog's last sentence is worthy of repetition and is a fine last thought for this FIPs history: "We are asking too much of the FIPs, yet they are far too entrenched and important to be abandoned."

## Appendix 1: Modernizing the 1980 OECD Statement of FIPs

In 2021, I proposed a revision for the Privacy Act of 1974.[95] As discussed above, Congress based that Act on the original version of FIPs as proposed by the HEW Advisory Committee. The 1974 Act did not include a statement of FIPs.

My proposed revision offered an adjustment to the original OECD FIPs version as part of the bill's statement of purposes. One reason for including a formal statement of FIPs was to stop the proliferation of FIPs versions by U.S. agencies. Another reason was to modernize the language of the OECD statement.

The report accompanying the revised Privacy Act of 1974 included a detailed explanation of the changes to the original OECD FIPs version. The changes did not seek to alter the original policy. Some of the changes adjusted the language of the OECD FIPs for a legislative format. Some changes made FIPs gender neutral. The FIPs revision also used *record keeper* rather *than data controller*, with *record keeper* being a more familiar term in the U.S, although not necessarily in the rest of the world.

Other changes called for more effort and more explanation. Not all of the language from 1980 matches up well with current privacy usage. Some language could be simplified while offering an identical principle. While some changes appear substantial on the surface, I repeat again that the goal was not to alter the original policy.

As a guide to anyone undertaking the task of updating the FIPs, I include here the section from the 2021 Privacy Act report that sets out the new FIPs language and the accompanying explanation of the modifications. The language here is from pages 52-56 of that report. I omitted the accompanying footnotes because they largely duplicate material that already appears here.

> Sec. 2. Findings and Purposes
>
> (a) FINDINGS. – The Congress finds that –
>
> *****

---

[94] See also Woodrow Herzog, *The Inadequate, Invaluable Fair Information Practices*, 76 Maryland Law Review 952 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3017312.

[95] Robert Gellman, From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974 (2021), https://www.worldprivacyforum.org/2021/05/from-the-filing-cabinet-to-the-cloud-updating-the-privacy-act-of-1974/. The paper is also at http://ssrn.com/abstract=3844965.

(7) reasonable implementation of the following principles of Fair Information Practices by Federal agencies will provide protections for individual privacy while allowing the Federal agencies to carry out their missions in an effective and efficient manner:
(A) the Principle of Collection Limitation provides that there should be limits to the collection of personally identifiable information, that the information should be collected by lawful and fair means, and that the information should be collected, where appropriate, with the knowledge or consent of the data subject;
(B) the Principle of Data Quality provides that personally identifiable information should be relevant to the purposes for which they are to be processed, and to the extent necessary for those purposes should be accurate, complete, and timely;
(C) the Principle of Purpose Specification provides that there must be limits to the processing of personally identifiable information and that the information should be processed only for the purposes specified at the time of collection and for compatible purposes;
(D) the Principle of Disclosure Limitation provides that personally identifiable information should not be disclosed except as provided under the purpose specification principle without the consent of the data subject or other legal authority;
(E) the Principle of Security provides that personally identifiable information should be protected by reasonable security safeguards against risks including loss, unauthorized access, destruction, use, modification, and disclosure;
(F) the Principle of Openness provides that the existence of record-keeping systems containing personally identifiable information be publicly known, along with a description of the record keeper, main purposes, uses, disclosures, policies, and practices for processing the information;
(G) the Principle of Individual Participation provides that individuals should have a right to see personally identifiable information about themselves and to seek amendment or removal of information that is not timely, accurate, relevant, or complete; and
(H) the Principle of Accountability provides that a record keeper should be accountable for complying with fair information practices.

The seventh finding emphasizes the importance of implementing Fair Information Practices in a reasonable manner that protects privacy and that also allows agencies to operate effectively and efficiently. The finding includes a complete statement of FIPs.

The background in Part II of this report describes the origins and importance of FIPs. I included a statement of FIPs in this bill because it is important that American law recognize a single version of FIPs. American law already mentions FIPs in various places, but there is no statement of FIPs in U.S. Code. One goal is to seek to end restatements and revisions of FIPs by federal agencies by having a congressional approved statement of the basic policy. More history of FIPs,

including many of the restatements of FIPs by federal agencies, can be found in a FIPs history that I maintain on my website.

This version in the bill originates with the highly influential version issued by the Organisation for Economic Cooperation and Development (OECD) in 1980. This statement of practices is general enough to serve the purpose to describing the broad policy goals of a privacy law while not unduly limiting activities that require the processing of personally identifiable information. FIPs remain a reliable and essential foundation for privacy policy and legislation.

Since I made some modifications to the OECD FIPs, I offer an explanation. None of the language changes seeks any substantive alteration to the original policies. Some wording changes adjust the language of the OECD FIPs for a legislative format. Some language changes make FIPs gender neutral. The draft also uses *record keeper* rather *than data controller*.

First, I replaced *personal data* with the bill's defined term *personally identifiable information*. This is the only change in the Collection Limitation Principle.

Second, in the Data Quality Principle, I replaced *up-to-date* with *timely*.

Third, the Purpose Specification Principle is reworded generally. The major change is to the original language that subsequent use be limited to the original purposes "or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose." The word *use* is difficult because it means *disclosure* in its original sense, but no longer has that meaning in modern privacy parlance. The concept of *incompatibility of purpose* raises what I call in the section above on Controlling Disclosure the *compatibility problem*. In place of the "not incompatible" language, I substituted "compatible purposes." I do not believe that this difference in wording is significant because none of these terms draws clear lines. That is a task for those who apply the principles.

Fourth, I renamed the Use Limitation Principle. It is now the Disclosure Limitation Principle. This change was essential because the bill defines use and disclosure in the modern privacy sense of the terms, a usage that postdates the original OECD version. This change does not seek to diminish the importance of limiting uses. That goal is fully met by the Purpose Specification Principle that information should be processed only for the purposes specified at the time of collection and for compatible purposes. There is, and always was, some overlap between these two principles.

Fifth, the Security Principle is unchanged but for the substitution of *personally identifiable information* for *personal data*.

Sixth, the Openness Principle is reworded somewhat, but the substance is the same as the OECD version.

Seventh, the Principle of Individual Participation confirms the right to see and to seek amendment of personally identifiable information. It offers less detail because the details seem out of place in a statement of principles and because a statement of basic rights implies (and the bill provides) due process with respect to these rights.

Finally, the Principle of Accountability is reworded, but the responsibilities of record keepers remain unchanged.

*****

## Version History for this Document

A note about sources and links: I try in this document to include as much text as possible rather than just links to original sources. Links go out of date faster than I can keep up. If a link is dead, you might try the Wayback Machine at https://web.archive.org/.

Version 1.5 adds a discussion about the restatement of FIPs in the report of the Privacy Protection Study Commission. 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.

Version 1.7 expands the discussion about the Department of Homeland Security's Fair Information Practice Principles. It also updates some links and lists the 10 Canadian Standard Association principles in a note.

Version 1.8 adds a brief discussion of the OECD 30th anniversary conference on the OECD Guidelines.

Version 1.81 adds a reference to the OECD 30th anniversary webpage.

Version 1.82 adds a brief discussion of the 2010 FTC staff report, revises the DHS discussion slightly, adds a discussion of the NSTIC FIPPs, and makes other mild revisions.

Version 1.83 adds a discussion of the June 2011 White House report on the energy grid.

Version 1.84 adds mention of an April 2011 OECD paper titled *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*.

Version 1.85 adds a paragraph on the 2009 Madrid Declaration.

Version 1.86 adds a paragraph on HIPAA and FIPs.

Version 1.87 adds a discussion of the February 2012 White House/Department of Commerce privacy report and Consumer Bill of Rights.

Version 1.88 adds a discussion of the 2012 FTC Report, of several HHS versions of FIPs, a bit of discussion of U.S. FIPs versions, clearer sectioning of the report, mild revisions here and there, as well as some minor additions to footnotes, updated links, and a slightly revised summary.

Version 1.89 fixes some typos and adjusts a statement or two.

Version 1.90 adds a paragraph in Part V on the Open Identity Exchange's Fair Information Practice Principles Comparison Tool.

Version 1.91 adds a biographical footnote, makes minor editorial changes, and fixes some dead links. Thanks to Eric Charikane for pointing out the problem. Keeping links current in a document like this is difficult.

Version 1.92 adds a discussion of EO 13636 and makes minor editorial changes.

Version 2.00 adds a discussion of the revised 2013 OECD Privacy Guidelines and makes minor editorial changes throughout (including changes to subsection numbering in Part IV). The reissuance of the OECD Privacy Guidelines is the justification for an increase in the revision number to the next major number. A subsection on recent history of FIPs, where discussion of the revised Guidelines appears, is new.

Version 2.01 adds a discussion of Marc's Rotenberg's speech at the OECD conference on the 30th anniversary of the guidelines.

Version 2.02 adds in a footnote a reference to a 1975 Massachusetts FIPs law and makes minor editorial changes here and there. The text box about FIPPs and FIPs is new with this version.

Version 2.1 updates to a new version of the Creative Commons License; adds links to transcripts of the 1972 HEW Committee that first proposed FIPs; includes a discussion of Graham Greenleaf's analysis of international privacy laws and standards; and revises the document's summary.

Version 2.11 adds Willis Ware's description of the origins of FIPs in an early footnote, a discussion of the February 2014 OMB Guidance for Providing and Using Administrative Data for Statistical Purposes, and fixes some typos. Always more typos!

Version 2.12 adds a reference to my article about Willis Ware and FIPs. It adds a discussion of the White House's 2014 Big Data reports. A discussion of the 2000 FTC report now offers more detail on the different versions of FIPs that the Commission identified in its 1998 and 2000 reports. The discussion of FIPs vs. FIPPS now includes a reference to the FTC's use of *principles* in connection with FIPs as early as 1998. Some links are updated.

Version 2.13 makes a modest number of minor edits and corrections to text, footnotes, and links.

Version 2.14 corrects typos and updates links. Thanks to Stephanie Perrin for finding the problems. I added a few new resources here and there and fixed some additional links.

Version 2.15 adds Paula Bruening's observation that FIPs are the common language of privacy, and adds, moves, and revises text in the last section.

Version 2.16 adds a discussion of the EU's GDPR, fixes some dead URLs, and made minor editorial adjustments. Thanks to Eric Charikane, PIAw@tch - The Privacy Impact Assessment Observatory, http://www.piawatch.eu, for prompting the update.

Version 2.17 adds a discussion of FIPs as found in OMB Circular A-130 (revised in 2016); adds a discussion of FIPs from a casebook by Mark Rotenberg and Anita Allen; fixes some dead links; and makes minor editorial adjustments and additions. It also adds the full text of the CSA Code as reflected in PIPEDA.

Version 2.18 corrects the date of enactment for the Minnesota Government Data Practices Act. Thanks for Bob Tennessen (the author of the Act and member of the Privacy Protection Study Commission) for pointing out the error.

Version 2.19 adds recollections about FIPs from Carole Parsons Bailey, who served as Associate Executive Director of the 1973 HEW Committee and as Executive Director of the 1975-77 Privacy Protection Study Commission; expands the quote (in an early footnote) from Willis Ware's discussion about the origins of FIPs; adds more information about and quotes from the Younger Committee Report in the UK in 1972; adds a discussion of the 2018 work of the Council of Europe on the CoE Convention 108; references a 2001 law journal article about FIPs by Marc Rotenberg and a more recent one from Woody Herzog; fixes and updates links.

Version 2.20 adds a discussion of Graham Greenleaf's paper mentioning "third-generation" privacy principles. It also adds a brief discussion of the statutory reference to FIPs in the Energy Act of 2020.

Version 2.21 adds a table of contents and a new Appendix 1 that reproduces language from another report that proposed a modest rewording of FIPs.

Version 2.22 adjusts the discussion of the 2008 ONC FIPs from the Department of Health and Human Services. Previous references to a speech by HHS Secretary Levitt as the source for the ONC FIP were removed and replaced by a better source. Thanks to Maya Bernstein for help here. There are also other minor language adjustments and link updates.