# FIPPs and PIA

From: **Peter Guffin** <PGuffin@pierceatwood.com>
Date: Thu, May 18, 2017 at 4:29 PM
Subject: FIPPs and PIA

Laura and Jack –

By way of follow up to the discussion at our last meeting, I have a few additional thoughts:

**Fair Information Privacy Practices (FIPPs)**

In crafting a high level statement of policy and principles ("Policy") to guide the Task Force in its work, I propose that we consider the FIPPs and incorporate them into the Policy, to the extent applicable.

The FIPPS are a collection of widely accepted principles that have been incorporated in the policies of many organizations around the world, including federal and state government agencies, and are applied by each organization to its particular mission and privacy program requirements when evaluating information systems, processes, programs, and activities that affect individual privacy. I've included in this email below some background information about the FIPPs that you may find helpful.

I think we should use the FIPPs as a reference point to guide us with respect to certain key issues, including the following:

Data minimization – the courts should limit collection of personally identifiable information (PII) to the minimum amount necessary for court purposes.

Notice – the courts should be transparent in describing the steps that they take to protect PII in court records. There should some assurance that the court will not sell PII in court records.

Access limitations – There is a presumption of public access to court records *where the purpose of access is related to public scrutiny of the judicial process*.

Use restrictions – PII in court records should be protected where the purpose of access is related to

commercial exploitation or potential misuse of the information with no public oversight purpose.

Enforcement – individuals should have the ability to petition the court for removal of their PII in court records.

I propose that the Policy include the following principle: the right of access to public court records is not absolute. When that right conflicts with an individual's right of privacy, the justification supporting the requested disclosure must be balanced against the risk of harm posed by the disclosure.

I also propose that that the Policy explicitly acknowledge the following realities:

· to fulfill its mission, the court system does, and often must, collect vast amounts of very sensitive PII

· individuals generally are not in a position to refuse providing this information to the court, so choice is not always an option for individuals

· potential privacy harms are much broader than just identity theft and credit card fraud, and include the risk of criminal offenses such as blackmail, extortion, stalking, bullying, and sexual assault. Public safety is a very compelling reason to protect PII

**Privacy Impact Assessment (PIA)**

I also recommend that we consider conducting and drafting a PIA.

A PIA is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

PIAs are widely used by all types of organizations around the world and are considered a very valuable tool to help ensure compliance with applicable privacy requirements and manage privacy risks.

In the U.S., for example, Section 208 of the E-Government Act (44 U.S.C. § 208 (2002)) requires all federal agencies to conduct a PIA whenever they develop a new technology involving the collection, use or disclosure of personal data. Under applicable OMB guidance for implementing the E-Government Act, PIAs are to identify and evaluate potential threats to individual privacy, identify appropriate risk mitigation measures and explain the rationale behind the final design choice.

I would be happy to expand on each of the above areas if you wish. Please let me know if you have any questions. Thank you.

Peter

The following background information about the FIPPs may be helpful.

**HEW Report**

In 1973, the U.S. Department of Health, Education & Welfare (HEW) issued a highly influential report about government records maintained in computer databases. The HEW Report, entitled *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, characterized the then growing concern over privacy in a way that was prescient:

> It is no wonder that people have come to distrust computer-based record-keeping operations. Even in non-governmental settings, an individual's control over the personal information that he gives to an organization or that an organization obtains about him, is lessening as the relationship between the giver and receiver of personal data grows more attenuated, impersonal, and diffused. There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays, an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers – unknown, unseen, and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others. . . .
>
> The poet, the novelist, and the social scientist tell us, each in his own way, that the life of a small-town man, woman, or family is an open book compared to the more anonymous existence of urban dwellers. Yet the individual in a small town can retain his confidence because he can be more sure of retaining control. He lives in a face-to-face world, in a social system where irresponsible behavior can be identified and called to account. By contrast, the impersonal data system, and faceless users of the information it contains, tend to be accountable only in the formal sense of the word. In practice they are for the most part immune to whatever sanctions the individual can invoke.

To remedy these growing concerns, the HEW Report recommended establishing a code of "fair information practices," intended to correct information asymmetries resulting from the transfer of personal data from an individual to an organization. The FIPPs assign rights to individuals and responsibilities to organization:

- There must no personal-data recordkeeping systems whose very existence is secret.

- There must be a way for an individual to find out what information about him is in a record and how it is used.

- There must be a way for an individual to prevent information about him that was 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 him.

- 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.

These FIPPs have played a significant role in framing privacy laws in the U.S, and these basic principles have also contributed to development of privacy laws around the world, including the development of important international guidelines.

The precise expression of the FIPPs has varied over time and in different contexts. However, the FIPPs retain a consistent set of core principles that are broadly applicable to organizations' information management practices.

**Circular A-130**

In the U.S., Office of Management and Budget (OMB) Circular A-130, titled Managing Information as a Strategic Resource, serves as the overarching policy and framework for all agencies of the Executive Branch of the Federal Government. Issued by the OMB in July 2016, Circular A-130 represents the most recent articulation of the FIPPs for federal government information resources management.

Circular A-130 defines the term PII as follows:

'Personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. It also is important to recognize that information that is not PII can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.

Circular A-130 expresses the FIPPs in this way:

a. *Access and Amendment*. Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

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.

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.

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.

**OECD Privacy Guidelines**

The most well-known of the international privacy guidelines are those issued in 1980 by the Organization for Economic Cooperation and Development (OECD), of which the U.S. is a member.

The OECD Privacy Guidelines "apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties." "Personal data" is defined as "any information relating to an identified or identifiable individual (data subject)."

The OECD Privacy Guidelines establish eight principles regarding the processing of personal data:

1. *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.

2. *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.

3. *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.

4. *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.

5. *Security Safeguards Principle.* Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. *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.

7. *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 (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) 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.

8. *Accountability Principle.* A data controller should be accountable for complying with measures which give effect to the principles stated above. . . .

The OECD Privacy Guidelines have had a significant impact on the development of privacy laws in the U.S. For example, the subscriber privacy provisions in the Cable Act of 1984 include many of the principles of the OECD Privacy Guidelines.

**Peter J. Guffin**
PIERCE ATWOOD LLP

Merrill's Wharf
254 Commercial Street
Portland, ME 04101

**PH** 207.791.1199
**FAX** 207.791.1350

PGuffin@pierceatwood.com

**BIO** ▸