DISCUSSION DRAFT

Privacy Act White Paper

Summary: This paper raises the question of whether the current legal and policy framework governing the information practices of Federal agencies are adequate to protect the privacy of individuals about whom the Federal government maintains or uses personal information. It postulates that laws and policies have not kept pace with changes in technology and information and handling processes and suggests the need for an open dialogue on what changes in law and policy are needed and how best to make those changes. The paper was prepared as a basis for a discussion by the Information Security and Privacy Advisory Board

The issues:

1. Is there a need to reopen the current legal and policy framework for managing information about individuals?
2. What role, if any, can the ISPAB play? Can we partner with others?

Background: The Privacy Act of 1974 initially enacted in 1974 establishes a general framework for protecting information about individuals maintained by Federal agencies. While the Privacy Act is the core of this discussion, it should be noted that Federal agencies are subject to a wide array of agency specific or subject matter specific laws that affect the gathering and use of personal information. The interplay between these laws and the Privacy Act may also be a subject for discussion.

The Privacy Act reflected the state of the technology and information practices at the time that it was considered and enacted, the early 1970s. Personal computers and networks as we know them today existed only in laboratories and software that allows us to associate data from disparate databases was not practicable. Moreover, emerging practices bolstered by these technologies, such as technology driven predictive analysis, were mostly confined to the private/commercial sector. Government databases that included personal data were operated largely by government employees. The Act did not contemplate any of these developments; indeed it was written in some instances specifically in terms of the then-existent technology.

While it is important to understand the historic context in which the political consensus emerged (i.e., Watergate and related events) that produced the Privacy Act, it is equally important to note that the Act was based on principles and analyses (intellectual capital if you will) that had been developed over at least a decade and beautifully synthesized in the seminal 1973 report Records, Computers and the Rights of Citizens. Thus when the political system was ready to act, much of the work had been done.

Even so, the Privacy Act was the result of compromise reached through an unusual method used to secure its passage. By late November 1974, both the Senate and House

had passed similar bills on the subject. But, because it was too late in the session to resolve the differences between these two bills through the standard process of a conference committee, an *ad hoc* group was formed comprised of Congressional staff and representatives from OMB and DOJ. This group considered the legislation for less than one month, developed a compromise bill that was passed by both houses on December 18, 1974 and signed into law on December 31, 1974. Critics contend that in their haste, this *ad hoc* group failed to consider all the possible ramifications of developing technologies, methodologies, governmental needs and the Act's interplay with other privacy regulatory mechanisms.

What has changed:

- Both the technology used to process data and the state of practice have changed materially in the past 30 years.

    - For example, the term "system of records" was defined to be a collection of records about individuals in which information was "retrieved by" individual identifier as opposed to "retrievable by." This language specifically and intentionally excluded systems in which an individual identifier might appear but was not used as a key word or organizing element so as not to require agencies to build the capacity to retrieve data by individual identifier. The existence of data mining software renders this distinction meaningless.
    - Similarly, the Act did not contemplate the extensive use of third party personal data by Federal agencies.
    - The development of sophisticated data mining techniques and other technologies has created greater need and desire for effective data matching programs that are more extensive than contemplated by the Act or the 1988 amendments.

- There is an increasing conflict between the goals of data minimization and the information needs of Federal Agencies.

- One criticism is that the Act's notice and access provisions are largely ineffective.

- Another criticism often raised is that the Act has no teeth.

    - Agencies broadly assert exemption from the Act; and
    - The remedies afforded in the Act are so weak that they are meaningless

Is there a need for action? One can argue that nothing in the Act prevents agencies from taking a broader view of the code of fair information practices embodied in the Act but the Act does not require it. Some agencies, most notably the Department of Homeland Security, have taken a broad view of their duty to protect the privacy of individuals about whom they collect maintain or access information, but they do so largely voluntarily. Of course the same argument could have been made, and was, prior to the enactment of the Act.

The arguments for change are two-fold:

- Absent changes in law or policy, some agencies will do the bare minimum
- A consistent, uniform framework makes it easier for the interested public to evaluate agency information practices and intervene where needed

Areas to consider:

- Definitions; e.g., system of records and individual
- Assuring data minimization
- Methods and vehicles for providing notice to data subjects
- Streamlining methods for data subject access to his/her records
- Providing adequate choice (in the G-to-C arena)
- Security/audit
- Remedies/enforcement
- The contractor provision
- The matching provisions as they apply (or do not) to use of third party data