

# Conceptual Proposal for a Joint Inquiry and Recommendations on a 21<sup>st</sup> Century Framework for Revisions to the Privacy Act of 1974 and Other Federal Privacy Statutes

This short paper outlines a conceptual proposal for a joint inquiry and recommendations on a 21<sup>st</sup> century framework for revisions to the Privacy Act of 1974 and related Federal privacy statutes to be undertaken by the Information Security and Privacy Advisory Board (ISPAB) and the Department of Homeland Security Data Privacy and Integrity Advisory Committee.

## Background

The **Information Security and Privacy Advisory Board (ISPAB)** is a federal advisory committee originally established by the Computer Security Act of 1987 (P.L. 100-35) as amended by the Federal Information Security Management Act of 2002 (P.L. 107-347) and managed by NIST. The membership of the Board consists of twelve members and a Chairperson. The Board meets quarterly throughout the year. The membership of the Board will include four members from outside the Federal Government eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries; four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

The scope and objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy; advising the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems; and reporting annually its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency and the appropriate committees of the Congress. The Board meets quarterly.

The **DHS Data Privacy and Integrity Advisory Committee (Privacy Advisory Committee)**, established under the authority of the Homeland Security Act, P.L. 107-296, advises the Secretary of the Department of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that affect individual privacy, as well as data integrity and data interoperability and other privacy related issues and recommends procedures that limit the re-dissemination of information to ensure that it is not used for an unauthorized purpose; ensure the security and confidentiality of information; protect the constitutional and statutory rights of any individuals who are subjects of such information; provide data integrity through timely removal and destruction of obsolete or erroneous names and information; monitor the use of data between DHS systems and between DHS systems and other Federal, state and local systems.

The Privacy Advisory Committee consists of 20 members appointed by the Secretary, and led by a Chair and Vice Chair. Membership is balanced among individuals currently working in the areas of higher education or research in public (except Federal) or not-for-profit institutions; individuals currently working in non-governmental industry or commercial interests, including at

least one representative of a small to medium enterprise; and other individuals, as determined appropriate by the Secretary. The committee meets quarterly.

### **Privacy Act Adequacy in 2005 and Need for Action**

Both advisory committees are addressing issues which touch on the applicability of the Privacy Act and related Federal government privacy requirements (such as the privacy impact assessments mandated by section 208 of the E-Government Act of 2002) to information systems now being designed and operated by DHS and other Federal agencies, in which information is collected, managed, disclosed and processed outside the apparent scope of the Privacy Act of 1974 and therefore impacting the applicability of privacy policies and controls across information system jurisdictions and boundaries.

For example, the use of commercial data, collected and aggregated for non-governmental purpose, but accessed by government systems for specific governmental functions, is arguably outside the scope of the Privacy Act. As a result, controls to ensure notice, disclosure, individual access and amendment which are required by the Privacy Act for government systems of records are not typically considered applicable to such private sector-sourced information.

These issues were addressed in the ISPAB's 2002 report, [Computer System Security and Privacy Advisory Board Findings and Recommendations on Government Privacy Policy Setting and Management](#)," and subsequent ISPAB work items. Likewise, they were directly addressed at the June 2005 meeting of the DHS privacy Committee [http://www.dhs.gov/dhspublic/interapp/editorial/editorial\\_0622.xml](http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0622.xml) (for example see the "Written supplement to oral testimony delivered on June 15, 2005: Recommended Policies for Use of Private Sector Data," submitted by the Center for Democracy and Technology).

Changes in technology over the past 31 years have made acute the privacy management challenges rising from the accelerated interaction of networked information systems within and across critical infrastructure boundaries, and the routine exchange of data among both Federal and non-Federal government and private sector systems. Given the charters of both the ISPAB and the DHS Privacy Committee, an examination of these issues and the development of a workable framework for revisions to the Privacy Act of 1974 is an appropriate joint effort for both committees, particularly given the interaction among DHS, non-DHS governmental and commercial information systems.

### **Proposal**

It is proposed that both the DHS Privacy Committee and the ISPAB consider a joint initiative to review the issues and develop a framework for revisions to the Privacy Act of 1974 and, as applicable, other Federal government privacy statutes and requirements, such as section 208 of the E-Government Act of 2002. This effort would be undertaken by a subcommittee formed by members of both committees, or parallel, well-coordinated subcommittees, in either case observing Federal Advisory Committee Act guidelines and requirements, and supported by both DHS and NIST to the extent deemed appropriate by the respective Designated Federal Officials and the Chairs of both committees.

It is recommended that the ISPAB and DHS Privacy Committee members consider this recommendation for joint action at their next quarterly meetings, and that the respective committee chairs and designated Federal officials determine the suitability of the joint activity under their respective committee charters.